Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Escuela de Ingeniería en Ciencias y Sistemas

CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS

Axel José Moscoso García

Asesorado por el Ing. Raúl Israel Canel Vásquez

Guatemala, julio de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

AXEL JOSÉ MOSCOSO GARCÍA
ASESORADO POR EL ING. RAÚL ISRAEL CANEL VÁSQUEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Narda Lucía Pacay Barrientos
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Marlon Antonio Pérez Türk
EXAMINADORA	Inga. Susan Verónica Gudiel Herrera
EXAMINADORA	Inga. Floriza Felipa Ávila Pesquera de Medinilla
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha febrero de 2015.

Axel José Moscoso García

Guatemala 11 de marzo de 2015

Ing. Carlos Azurdia
Revisor de Trabajos de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Respetable Ing. Azurdia:

El motivo del presente es para saludarlo y que todas sus actividades profesionales le sean de éxito.

Hago de su conocimiento que he revisado el trabajo de graduación realizado por el estudiante **Axel José Moscoso García** con número de carnet **95-16262** titulado "**Controles sobre los recursos tecnológicos con que cuenta la organización para prevenir situaciones no deseadas y corregirlos**", y a mi criterio el mismo cumple con los objetivos propuestos, según el protocolo.

Sin otro particular, me suscribo de usted.

Atentamente,

Ing. Raúl Israel Canel Vásquez

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 27 de Mayo de 2015

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **AXEL JOSÉ MOSCOSO GARCÍA** con carné **1995-16262,** titulado: **"CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TESIS

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS",*** *realizado por el estudiante AXEL JOSÉ MOSCOSO GARCÍA, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pérez Türk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 17 de julio de 2015

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.D.351.2015

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **CONTROLES SOBRE LOS RECURSOS TECNOLÓGICOS CON QUE CUENTA LA ORGANIZACIÓN PARA PREVENIR SITUACIONES NO DESEADAS Y CORREGIRLOS,** presentado por el estudiante universitario: **Axel José Moscoso García,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, julio de 2015

/cc

ACTO QUE DEDICO A:

Dios	Por ser el Rey de Reyes y Señor de mi vida y darme la sabiduría y fuerza necesaria para llegar a cumplir esta meta.
Mis padres	José Ladislao Moscoso Cardona y Martha Angélica García Zuleta, por todos sus sacrificios, consejos y cariño para que pudiera alcanzar esta meta; este triunfo es para honrarles.
Mi esposa	Linda Ivette Carrillo Ramos de Moscoso. Gracias por tu paciencia y apoyo para alcanzar esta meta.
Mis hijos	Diana y Axel Moscoso Carrillo. Son una bendición y fuente de inspiración para mi vida.
Mis hermanos	Marlon y Claudia Moscoso García, por su apoyo espiritual moral e incondicional; porque me han dado fuerza para alcanzar este éxito.
Mis familiares	Con cariño sincero, muchas gracias a todos.
Mis amigos	Gracias por brindarme su amistad y confianza en todo momento.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser el alma máter al estudiar esta carrera universitaria.
Facultad de Ingeniería	Por permitirme ser el fruto del saber.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

Auditoría Es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.

Asp Del inglés active server pages; es una tecnología de Microsoft del tipo "lado del servidor" para páginas web generadas dinámicamente, que ha sido comercializada como un anexo a *Internet Information Services*.

Dns Del inglés domain name system; es una tecnología que utiliza base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que se quiere acceder.

Dhcp Del inglés dynamic host configuration protocol; es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular).

Malware Es una categoría de códigos maliciosos que incluye virus y troyanos. El *malware* destructivo usará herramientas de comunicación popular para extenderse, incluyendo gusanos troyanos enviados a través de *e-mails* y mensajes instantáneos que entran a través de páginas web y archivos infectados por virus descargados en conexiones directas entre usuarios. El *malware* buscará la manera de explotar las vulnerabilidades del sistema, entrando de un modo silencioso y sencillo.

Phishing Es básicamente un fraude online, y los *phishers* no son más que estafadores tecnológicos. Estos utilizan *spam*, páginas web fraudulentas, *e-mails* y mensajes instantáneos, para hacer que las personas divulguen información delicada como información bancaria y de tarjetas de crédito, o acceso a cuentas personales.

Proxy Es un servidor, programa, que sirve de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C).

Proyecto Es un conjunto articulado de actividades orientadas a alcanzar uno o varios objetivos, para lo cual precisa de un equipo de personas idóneas, así como de otros recursos cuantificados en forma de presupuesto para desarrollar determinados resultados, y cuya programación en el tiempo

responde a un cronograma con una duración limitada.

Raid — Del inglés *Redundant Array of Independent Disks*; es un método de combinación de varios discos duros para formar una única unidad lógica en la que se almacenan los datos de forma redundante. Ofrece mayor tolerancia a fallos y más altos niveles de rendimiento que un disco duro o un grupo de discos duros independientes.

Spam — Es la versión electrónica del correo basura. Conlleva el envío de mensajes indeseados, a veces publicidad no solicitada, a un gran número de destinatarios. El *spam* es un asunto serio de seguridad, ya que puede usarse para entregar *e-mails* que puedan contener troyanos, virus, *spyware* y ataques enfocados a obtener información personal delicada.

Spyware — Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

Virus — Es un programa malicioso (*malwares*) que infecta a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo víctima (normalmente un ejecutable), de forma que a

partir de ese momento, dicho ejecutable pasa a ser portador del virus y por tanto de una nueva fuente de infección.

RESUMEN

Los controles protegen los recursos de la organización, buscando una adecuada administración ante riesgos potenciales y reales que los puedan afectar, así garantizar la eficiencia, eficacia y economía en todas las operaciones de la organización, promoviendo y facilitando la correcta ejecución de las funciones y actividades establecidas. En la actualidad las empresas deben renovar con mayor frecuencia sus ventajas competitivas mediante la innovación y movilización de todos sus recursos tecnológicos, por lo que es necesario tener controles sobre los mismos.

Los cambios tecnológicos ocurren tan rápido que no se ha terminado la asimilación de la última tecnología y ya aparece otra. Los mercados se tornan muy competitivos y para poder insertarse en ellos es necesaria la innovación constante como la única estrategia de supervivencia para la organización.

El análisis de riesgos tiene como resultado los informes de recomendaciones de seguridad, para que la organización pueda evaluar los riesgos a que está sometida y conocer cuáles son los activos de los procesos de negocio que están más susceptibles a la acción de amenazas a la confidencialidad, integridad y disponibilidad de la información utilizada, para alcanzar los objetivos intermedios o finales de la organización.

Las organizaciones pueden verse sorprendidas en cualquier momento por la aparición de nuevos productos, nuevas tecnologías, nuevos competidores o cambios en los gustos de los clientes, que pueden amenazar seriamente la buena marcha de la empresa.

El análisis estratégico requiere que mediante el análisis externo se detecten las oportunidades y amenazas a las que la empresa se enfrenta como consecuencia de las situaciones del entorno en el que opera; es necesario efectuar el análisis interno de los recursos y competencias que la empresa posee; asimismo un diagnóstico y evaluación de sus recursos.

El control estratégico tratará de facilitar el seguimiento de las acciones internas y externas de la organización, las cuales le van a permitir alcanzar los objetivos deseados con base en las estrategias desarrolladas.

OBJETIVOS

General

Garantizar el funcionamiento correcto de la empresa con información íntegra, eficiente, disponible, confidencial y eficaz, teniendo en cuenta los recursos tecnológicos, humanos y la aplicación para prevenir situaciones no deseadas desde el punto de vista hardware, software, comunicación e información.

Específicos

1. Establecer qué son y para qué sirven los recursos tecnológicos dentro de la organización.

2. Enunciar la importancia de tener controles sobre los recursos tecnológicos y humanos e información en la organización.

3. Definir la importancia del uso adecuado del recurso tecnológico.

4. Establecer la importancia en identificar y analizar los riesgos informáticos.

5. Identificar de qué forma la tecnología de información puede contribuir para la obtención de los objetivos del negocio.

6. Garantizar que los objetivos de la empresa serán alcanzados y que eventos no deseables serán prevenidos.

7. Establecer un plan de administración y actualización de hardware y software.

8. Medir el impacto financiero de los recursos tecnológicos.

INTRODUCCIÓN

Las organizaciones están cambiando profundamente a la creciente del desarrollo tecnológico, la globalización de los mercados y la economía; tal situación pone de manifiesto la progresiva incorporación dentro de las empresas el uso de tecnología de información y telecomunicaciones. Las nuevas tecnologías están incidiendo en gran medida sobre los puestos de trabajo, estructura organizacional, procesos y gestión organizacional y las relaciones de la propia organización en su entorno.

Los controles permiten conformar un ambiente eficaz de tecnología de la información, a través del cual se procese y obtenga información confiable para la organización y se logre el funcionamiento de los procesos del negocio. Las organizaciones deberían disponer de herramientas de control que les permita analizar y detectar los usos y comportamientos indebidos o ilícitos en los recursos, los cuales puedan suponer un riesgo en la seguridad de los sistemas de la empresa.

Las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben estar conscientes de que la administración del riesgo informático juega un rol crítico, donde los sistemas de información son vulnerables a una diversidad de amenazas y atentados por parte de personas tanto internas como externas de la organización. Las amenazas surgen a partir de la existencia de vulnerabilidades; es decir que una amenaza solo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

El impacto que produce la amenaza en la organización no depende de las características de la vulnerabilidad, sino del grado de criticidad de la parte del sistema informático en que puede llegar a actuar.

El análisis tiene como objetivo identificar los riesgos mediante la identificación de sus elementos y establecer el riesgo total o exposición bruta al riesgo y luego el riesgo residual, ya sea en términos cuantitativos o cualitativos. Al tener los resultados del análisis de riesgos, la organización tiene en sus manos una poderosa herramienta para el tratamiento de sus vulnerabilidades y un diagnóstico general sobre el estado de la seguridad de su entorno como un todo.

Las organizaciones, dependiendo de la orientación del negocio, difieren en sus regímenes tecnológicos. Cada sector involucra distintas tecnologías, las cuales presentan una ruta histórica de desarrollo diferente y requerimientos estratégicos particulares. El éxito de una empresa intensiva en la tecnología depende de manera decisiva de su base tecnológica, es decir, de su capacidad para explorar y explotar la tecnología como una competencia medular, incorporar tecnología más avanzada en productos y servicios, y hacerlo en un período menor, con costos inferiores y con mayor rendimiento que los competidores.

1. CONTROLES Y RECURSOS TECNOLÓGICOS

1.1. Definición de controles

Control es el mecanismo para comprobar que las cosas se realicen como fueron previstas, de acuerdo con las políticas, objetivos y metas fijadas previamente para garantizar el cumplimiento de la misión organizacional.

El control está definido como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer una seguridad razonable que los objetivos de la organización serán alcanzados.

El control es una etapa primordial en la administración, aunque una empresa cuente con magníficos planes, una estructura organizacional adecuada y una dirección eficiente; no se podrá verificar cuál es la situación real de la organización si no existe un mecanismo que se cerciore e informe si los hechos van de acuerdo con los objetivos.

El control es un factor importante para el logro de los objetivos de la organización y por ello debe reunir ciertas características para ser efectivo. El control deberá ajustarse a las necesidades de la empresa y al tipo de actividad que se desee controlar. Los buenos controles deben relacionarse con la estructura organizativa y reflejar su eficacia.

Los controles permiten conformar un ambiente eficaz de tecnología de la información, a través del cual se procese y obtenga información confiable para la organización y se logre el funcionamiento de los procesos del negocio.

Los controles ayudan a reducir los riesgos o amenazas que pueden tener un impacto negativo sobre sus activos, procesos u objetivos de la organización.

Los controles protegen los recursos de la organización, buscando una adecuada administración ante riesgos potenciales y reales que los puedan afectar, para garantizar la eficiencia, eficacia y economía en todas las operaciones de la organización, promoviendo y facilitando la correcta ejecución de las funciones y actividades establecidas. En la actualidad las empresas deben renovar con mayor frecuencia sus ventajas competitivas mediante la innovación y la movilización de todos sus recursos tecnológicos, por lo que es necesario tener controles sobre los mismos.

1.2. Definición de recursos tecnológicos

Un recurso son todos aquellos elementos que permiten satisfacer necesidades o alcanzar objetivos. Los recursos tecnológicos son medios con los que se vale la tecnología para cumplir su propósito; sirven para optimizar procesos, tiempos, y recurso humano, agilizando el trabajo y tiempos de respuesta que finalmente impactan en la productividad y muchas veces en la preferencia del cliente o consumidor final. Los recursos tecnológicos considerados se clasifican como tangibles e intangibles.

Los recursos tangibles son aquellos que pueden ser percibidos físicamente (vistos, tocados o medidos); contar con los recursos tangibles adecuados es un elemento clave en la gestión de las organizaciones. Los recursos tangibles pueden ser herramientas, equipos, instrumentos, materiales, máquinas, dispositivos y software específicos necesarios para lograr el propósito técnico establecido.

Figura 1. **Recursos tangibles**

Fuente: *Cero inventarios, sí, pero…… ¿a cualquier precio?.* http://www.eoi.es/blogs/madeon/2013/03/13/cero-inventarios-si-pero%E2%80%A6%E2%80%A6-%C2%BFa-cualquier-precio-4/. Consulta: 10 de febrero de 2015.

Los recursos intangibles son aquellos recursos distintos de los financieros, que no pueden ser percibidos físicamente; es muy difícil estimar o cuantificar el impacto de los mismos en los resultados de la organización. Los recursos intangibles pueden ser identificados como capital intelectual (estructural y humano) o de manera más general como información y conocimiento.

Figura 2. **Recursos intangibles**

Fuente: *Creación de conocimiento*. http://sites.google.com/site/groupccygv/wiki-del-proyecto/1-las organizaciones-como-generadoras-de-conocimiento-1/2-1-creacion-de-conocimiento. Consulta: 10 de febrero de 2015.

1.2.1. Información

La información es todo aquel conjunto de datos organizados que permiten saber sobre determinada cosa, evento o fenómeno; dentro de la información se pueden encontrar datos que describan físicamente un objeto, así como también su origen, sus usos, su historia.

La información es un conjunto organizado de datos a los que se les ha dado una forma que tiene sentido, que constituyen un mensaje que cambia el estado del conocimiento del sujeto o sistema que recibe dicho mensaje.

La información es el significado que se le da a los datos, una vez que han sido clasificados y procesados; o sea que para obtener información hay que recibir los datos, analizarlos, trabajar sobre ellos y presentarlos en forma tal que puedan servir para obtener conclusiones o tomar decisiones.

La función de la información es el poder aumentar el conocimiento de las personas que tienen sobre algo, lo que en algunos casos puede ayudar en la toma de decisiones y en la evaluación de determinados procesos, hecho, personas o cosas.

La información es una herramienta muy valiosa, ya que se puede dirigir cualquier situación que se requiera, para una mejora en los diferentes aspectos de la organización.

La información puede considerarse a su vez como un recurso básico en la gestión empresarial; sin ella los directivos tienen que actuar de manera intuitiva.

Figura 3. **Información**

Fuente: *Valoración sobre el derecho de acceso a la información*. http://rendiciondecuentas.org.mx/valoracion-sobre-el-derecho-de-acceso-a-la-informacion/. Consulta: 10 de febrero de 2015.

1.2.2. Servidor

El servidor es un equipo informático que forma parte de una red y que provee servicios a otros equipos denominados clientes. El servidor es la computadora encargada de almacenar y hacer disponible la información electrónica publicada por el centro de datos.

1.2.2.1. Hardware

El hardware es la parte física de un ordenador o sistema informático, está formado por los componentes eléctricos, electrónicos, electromecánicos y mecánicos, tales como circuitos de cables, circuitos de luz, placas, utensilios, cadenas y cualquier otro material en estado físico que sea necesario para hacer que el equipo funcione.

Un servidor es un proceso que entrega información o sirve a otro proceso; es muy probable que un ordenador cumpla simultáneamente las funciones de cliente y de servidor al mismo tiempo; un caso muy común son los equipos que funcionan como servidor web, servidor ftp y servidor de correo. Aunque

normalmente se suele hacer distinción entre cada uno de ellos y se utiliza un solo equipo para cada servicio, dependiendo el tamaño de la red y las exigencias de la misma.

Lo que diferencia a los servidores de las PC es su rendimiento, disponibilidad y frecuencia de fallos de hardware. Un servidor debe estar encendido 24 horas al día, 365 días al año; debe soportar en ciertos instantes alta realización de procesos y mantener una temperatura estable para que sus componentes funcionen de forma óptima en todo momento y su tiempo de respuesta no sea afectado.

Figura 4. **Servidor**

Fuente: *Componentes de un sistema de cómputo*. http://problemasconlatecnologia.blogspot.com/2013/06/322-componentes-de-un-sistema-de.html. Consulta: 10 de febrero de 2015.

En un servidor es normal encontrar otras características especiales con su hardware como fuente de poder redundante, discos RAID, doble procesador y unidades de cinta.

Al momento que la organización va a adquirir un servidor, debe tener en cuenta el crecimiento de la institución en cuanto a servicios y productos, documentos digitalizados, cuentas de correo, base de datos y el licenciamiento del software para cada uno de sus servicios cuando aplique.

1.2.2.1.1. Funciones del servidor

La función de un servidor es proveer servicios a otras computadoras conectadas en red, llamadas clientes. A continuación se lista una serie de funciones de un servidor:

- Administrar y controlar sitios web, incluyendo los productos y servicios que este alberga.
- Administrar los servicios de red que se utilizan dentro de la organización: administración de impresoras compartidas, acceso a internet, servicios de archivos, proxy, acceso remoto, autenticación, DNS, DHCP, etc.
- Implementar procedimientos para tener la información respaldada.
- Proteger la red de los virus informáticos.
- Administrar los sistemas de correo electrónico, base de datos.

1.2.2.2. Software

El software es la información codificada que es transmitida al hardware para que este la procese y la ejecute.

El software necesita del hardware para poder funcionar, ya que este le provee de los recursos necesarios como procesador, memoria, espacio en disco duro, etc. para poder hacerlo correctamente.

El software también puede ser clasificado según su distribución y tipo de licencia. Hay 2 grandes clasificaciones para el software las cuales son: software propietario y software libre.

- Software propietario: es el que generalmente se comercializa y es del conocimiento de todos. Para citar un ejemplo se puede mencionar a *Microsoft*® que distribuye Microsoft Office o Microsoft Windows de forma propietaria. Esto quiere decir que una vez que se adquieren estos productos se tienen derechos muy limitados sobre él; en este caso no se podría copiar, modificar ni mucho menos redistribuirlo, salvo autorización explícita del dueño de los derechos. El software privado también es conocido como privativo, privado, de código cerrado, cautivo o software no libre.

- Software libre: es el que respeta las libertades del usuario sobre el producto adquirido, por lo que la FSF (*Free software foundation*) define que una vez adquirido el software este puede ser ejecutado, copiado, distribuido, estudiado y aún modificado con total libertad. Generalmente el software libre es distribuido gratuitamente o a costos realmente accesibles pero no tiene por qué ser así siempre; este se puede comercializar como cualquier otro software.

  Como anotación, al software que se distribuye totalmente gratis se le llama *freeware*. Este tipo de software ha tenido mucho auge y popularidad en este último tiempo, ya que le da muchas más libertades al usuario que el software propietario o privativo. Algunos ejemplos de programas de esta clasificación estarían Linux Ubuntu, Libre Office, Mozilla y Firefox.

Figura 5. **Aplicaciones de software propietario y software libre**

Fuente: *Ejemplos de software libre y propietario*. http://serap97.wordpress.com/. Consulta: 11 de febrero de 2015.

1.2.2.2.1. Sistema operativo

Sistema operativo (SO) es aquel programa o software encargado de administrar y gestionar los recursos disponibles de un ordenador a nivel de hardware, y proporciona el correcto ambiente para que el usuario pueda ejecutar programas.

La función principal del sistema operativo es la de proporcionar las herramientas necesarias para controlar la computadora y hacer uso de ella. Los sistemas operativos no son de uso exclusivo de las computadoras sino que también se utilizan para controlar e interaccionar con los teléfonos celulares, *tablets*, *routers*, reproductores de DVD, consolas de videojuegos, radios y otros.

Existe un gran número de distribuciones libres y comerciales que proporcionan las funcionalidades que necesita un servidor, por lo que varias de ellas pueden ser adecuadas de acuerdo con los objetivos y políticas de la organización.

- Sistema operativo Microsoft Windows:
    - En sus diferentes versiones, Microsoft Windows es el sistema operativo más ampliamente usado.
    - La adquisición del sistema operativo brinda el servicio de soporte técnico y actualizaciones por un período limitado (generalmente, de un año) y debe ser renovado al cabo de este plazo.
    - Es un producto propietario de Microsoft por el que se debe pagar.
    - Existen diferentes planes de soporte técnico con diferentes niveles de servicios y costos.
    - Windows incluye una herramienta de actualización automática que permite corregir errores y debilidades de seguridad. Sin embargo, la actualización a una nueva versión implica un costo y, usualmente, nuevos términos de licencia.

- Sistema operativo Linux:

    - Pertenece a una familia de tecnologías de código abierto (*open source*) que surge como una alternativa a los productos Microsoft.

    - Existen distribuciones (“distros”) que pueden ser adquiridos gratuitamente desde la web y distribuciones comerciales que tienen un costo (generalmente, menor que el de los productos de Microsoft).

    - Una distribución de Linux es una línea de desarrollo del producto, elaborada y mantenida por una comunidad de programadores.

    - Hay gran número de distribuciones distintas de Linux. Cada una tiene un conjunto de herramientas y capacidades que pueden variar de una distribución a otra. Por ejemplo, algunas distribuciones de Linux tienen interfaces de usuarios diferentes; otras están orientadas a tareas específicas como seguridad de la información, la implementación de servidores, etc.

    - Las comunidades de usuarios de Linux mayormente proporcionan el soporte técnico de forma voluntaria. Además, es posible contratar el servicio de soporte de compañías técnicas comerciales.

    - Algunas distribuciones de Linux incluyen herramientas de actualización automática que permiten corregir errores y problemas de seguridad, e incluso, a diferencia de Microsoft

Windows, permiten la actualización a nuevas versiones del sistema operativo sin costo adicional.

Figura 6. **Diferentes sistemas operativos**

Fuente: *Que es un sistema operativo*. http://tecnomisterio15.blogspot.com/. Consulta: 11 de febrero de 2015.

1.2.2.2.2. Software administrador de servicios web

Un servidor web es un programa que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de internet. El servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web o información de todo tipo, de acuerdo con los comandos solicitados. El servidor web consta de un intérprete HTTP (*hypertext markup language*), el cual se mantiene a la espera de peticiones de clientes y le responde con el contenido, según sea solicitado. El cliente, una vez recibido el código, lo interpreta y lo exhibe en pantalla.

El servidor web puede disponer de un intérprete de otros lenguajes de programación que ejecutan código embebido dentro del código HTML de las páginas que contiene el sitio, antes de enviar el resultado al cliente. Esto se conoce como programación de lado del servidor y utiliza lenguajes como ASP, PHP, Perl y Ajax. Las ventajas de utilizar estos lenguajes radican en la potencia de los mismos, ejecutando tareas más complejas como por ejemplo acceder a bases de datos, abstrayendo al cliente de toda la operación.

- *Internet information server* (IIS):

    - Es un sistema administrador de servicios web propietario de Microsoft que solo trabaja sobre servidores Windows.

    - Incluye una interfaz de administración altamente gráfica y de fácil utilización.

    - Cuenta con el respaldo técnico y garantía de Microsoft Corporation.

    - Algunas aplicaciones desarrolladas para ejecutarse en otros sistemas administradores de sitios web podrían no funcionar en IIS.

    - Dispone de una arquitectura completamente modular que funciona a partir de API de extensibilidad, así es fácil agregar o quitar componentes.

    - Es un producto comercial.

- Ofrece un mayor aislamiento de la aplicación, ya que proporciona a los procesos de trabajo una identidad única y una configuración de espacio aislado de forma predeterminada.

- Apache Web Server:

  - Es un sistema multiplataforma gratuito que puede ser instalado en servidores Windows o Linux.

  - Por lo general, la administración de Apache requiere un trabajo más detallado y un nivel mayor de conocimientos técnicos.

  - La interfaz de administración no es generalmente gráfica.

  - El servidor Apache permite un alto grado de flexibilidad, funcionalidad y rendimiento.

  - Puede ser adaptado a diferentes módulos.

  - Es un producto libre.

  - Cuenta con el apoyo de las comunidades de programadores y usuarios.

  - Es muy portable, se puede instalar en una amplia variedad de servidores y sistemas operativos; es capaz de ejecutarse en todas las versiones de sistemas operativos Unix, Linux, Windows y MacOS.

- Debe tener en consideración que algunas aplicaciones desarrolladas para ejecutarse en otros sistemas administradores de sitios web podrían no funcionar en Apache.

1.2.2.2.3. Software servidor de correo electrónico

El servidor de correo electrónico es un producto de software que permite la habilitación del servicio de correo electrónico.

Permite una buena administración de la seguridad y privacidad de los correos electrónicos, garantizando la fiabilidad de los datos e incrementando el rendimiento en el proceso de sincronización de mensajes.

El servidor de correo permite el manejo de múltiples dominios, donde se administran listas de correo, alias y usuarios virtuales; se debe de tener un excelente control de acceso.

El servidor de correo realiza una serie de procesos que tienen la finalidad de transportar información entre los distintos usuarios.

- Microsoft Exchange Server exclusivo para Microsoft Windows: es un producto comercial, cuenta con el soporte técnico de Microsoft Corporation, es de fácil instalación y administración, ofrece una amplia gama de opciones de despliegue, facilidad de acceso a los buzones para los usuarios finales, incorpora un sistema de filtro anti-spam avanzado, basado en análisis de la conexión, emisor, receptor y contenido, para bloquear los mensajes no deseados y protegerse frente a ataques de *phishing*.

- HmailServer: trabaja sobre Microsoft Windows, es un producto gratuito y de código abierto, cuenta con el apoyo de programadores y usuarios, la instalación es rápida, añade flexibilidad y seguridad que le da el control total sobre la protección contra el spam, filtrando el correo según su procedencia o contenido; permite administrar el correo de uno o varios dominios.

- SendMail: trabaja sobre Unix y Linux, es un producto libre, cuenta con el apoyo de programadores y usuarios, la instalación requiere mayor trabajo y conocimiento, puede ser configurado para evitar mensajes spam no deseados para cualquier persona que reciba correo electrónico a través del sistema.

Una opción económica y que no requiere de un servidor instalado en la organización es la externalización de los servicios de correo electrónico. Por ejemplo, existen compañías como Gmail versión empresarial y Outlook *online* que proporcionan este servicio.

1.2.2.2.4. Software de respaldo

El software de respaldo permite administrar y controlar diversas copias de archivos digitales importantes en diversos tipos de dispositivos de almacenamiento (cintas, discos duros externos, entre otro.). Es efectivo si sigue estrictamente los procedimientos de seguridad y mantenimiento de la información establecida por la institución.

- CA ArcServer Backup:
    - Es un sistema comercial que trabaja sobre plataformas Microsoft Windows, Linux, NetWare y Unix.

- Permite una gestión centralizada a través de una consola.

- Ofrece una protección de datos de fiabilidad empresarial a través de múltiples plataformas software y hardware, permitiendo una protección multicapa.

- Mejora el rendimiento y la fiabilidad a través de la integración con cintas de respaldo o de disco a disco.

- Brinda protección contra los virus informáticos, incluyendo procesos de encriptación.

- Permite preparar rápidamente a responder y recuperar ante desastres e interrupciones, para mantener la integridad y fiabilidad de las operaciones de la organización.

- FBackup:

  - Es un sistema libre de costo.

  - Trabaja sobre plataforma Microsoft Windows.

  - Permite al usuario controlar múltiples destinos de copias de respaldo, comprimir la información, generar copias de archivos abiertos y actualizarse en forma automática.

  - Tiene una interfaz sencilla y lo guía a través del proceso de definir tareas de respaldo usando un asistente amistoso, donde podrá indicarle si lo desea realizar manual o automáticamente.

- La restauración es sencilla de usar, solamente hay que elegir la ubicación donde se desean recuperar los archivos copiados y elegir cuáles son los que se restaurarán, que pueden ser todos, o por el contrario, solo algunos de ellos.

- Clonezilla:

  - Es un software libre de recuperación ante desastres.

  - Es una herramienta para realizar copias de seguridad de discos duros, independientemente del sistema operativo que contenga.

  - Permite la realización de imágenes de discos, para luego restablecerlas en otra computadora.

  - El software se puede ejecutar ya sea desde un arranque de unidad flash USB o CD/DVD.

1.2.2.2.5. Software *firewall*

El *firewall* es un filtro de seguridad que controla todas las comunicaciones electrónicas que pasan por una red. Permite o bloquea cierto tráfico de acuerdo con las normas de seguridad establecidas, también conocido con muro de fuero. Este software ayuda, por ejemplo, a evitar el acceso ilícito a los recursos electrónicos del centro de datos (*hackers*) o el uso indebido de algunos recursos tecnológicos. Este proceso de filtrado se realiza sobre servicios electrónicos como acceso a sitios web, correo electrónico, mensajería instantánea y transferencia de archivos (FTP), entre otros.

El *firewall* se utiliza con frecuencia para evitar que los usuarios de internet no autorizados tengan acceso a redes privadas conectadas a internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del *firewall*, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

El *firewall* correctamente configurado añade una protección necesaria a la red, la cual en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

El *firewall* no puede proteger contra aquellos ataques cuyo tráfico no sea a través de él. No puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. No puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas de la organización. No puede proteger contra los ataques posibles a la red interna por virus informáticos a través de archivos y software.

- ISA Server:

    - Es un sistema comercial que trabaja sobre plataforma Microsoft Windows.

    - Protege los sistemas de amenazas procedentes de internet, permitiendo a los usuarios acceder en forma remota y segura a sus aplicaciones y datos corporativos.

    - Existen dos versiones: ISA Server Edición Estándar e ISA Server Edición Enterprise.

- Permite que las organizaciones puedan disponer de acceso a sus servidores Exchange, SharePoint u otras aplicaciones web de forma segura, desde fuera de la red corporativa.

- Cómodo *Firewall*:

  - Es un sistema libre de costo que trabaja sobre plataforma Microsoft Windows.

  - Permite proteger el sistema ante ataques de virus informáticos, troyanos, *hackers* y otros, controlando en detalle las aplicaciones que tienen acceso a internet a través de reglas de acceso y del monitoreo constante de su comportamiento.

  - Ayuda a proteger la computadora de conexiones no autorizadas hacia y desde internet.

- Netfilter/iptables: es un *framework* disponible en el núcleo de Linux que permite interceptar y manipular paquetes de red, ofrece infraestructura flexible y extensible y permite definir políticas de filtrado.

1.2.2.2.6. Software antivirus

El antivirus es un software que se encarga de detectar, detener y eliminar la mayor cantidad de amenazas de virus informáticos que puedan afectar el servidor. Para ello monitorea permanentemente todos los archivos abiertos, creados, modificados, ejecutados y transmitidos mientras el servidor trabaja.

El antivirus es un programa que funcionará correctamente si es adecuado y está bien configurado. Además, un antivirus es una herramienta para el usuario y no será eficaz para todos los casos, sino que nunca será una protección total ni definitiva.

Los virus informáticos son programas de software concebidos expresamente para interferir en el funcionamiento del equipo, registrar, dañar o eliminar datos, o bien propagarse por otros equipos y a través de internet.

Los virus más comunes son los troyanos y gusanos, los cuales ocultan la información, creando accesos directos.

El antivirus debe ser actualizado frecuentemente, pues con tantos códigos maliciosos siendo descubiertos todos los días, los productos pueden hacerse obsoletos rápidamente. Algunos antivirus pueden ser configurados para que se actualicen automáticamente.

- ESET NOD32:

    - Es un sistema comercial que trabaja sobre plataforma Microsoft Windows y Linux.

    - Permite analizar los archivos a gran velocidad con una alta tasa de detección de virus informáticos.

    - Optimiza el consumo de los recursos del servidor y brinda la posibilidad de analizar archivos en formato comprimido (ZIP, RAR, ARJ, LZH, LHA, CAB, CHM, TAG, GZIP).

- Brinda protección contra un amplio espectro de códigos maliciosos: virus, gusanos, troyanos *spyware* y otros ataques malignos, en constante evolución.

- Garantiza un rápido arranque del sistema y no causa problemas en el rendimiento del ordenador.

- ClamAV:

  - Es un sistema gratuito y de código abierto que trabaja sobre plataforma Linux, Windows, Solaris y Mac OS X.

  - Incluye análisis de correo electrónico.

  - Uno de los puntos fundamentales en este tipo de software es la rápida localización e inclusión en la herramienta de los nuevos virus encontrados y escaneados.

  - Se desarrolla gracias a una red de contribuidores que proporcionan parches, información de *bugs*, soporte técnico y documentación.

1.2.2.2.7. Software de monitoreo de la red

El sistema de monitoreo de la red permite visualizar la actividad en la red, identificando las computadoras y periféricos conectados, la disponibilidad y rendimiento de la red y los protocolos de comunicación (HTTP, SMTP, FTP, DNS, POP3, etc.) utilizados en la red.

Es un sistema que constantemente monitorea una red de computadoras en busca de componentes defectuosos o lentos, para luego informar a los administradores de redes mediante correo electrónico y alarmas, generando estadísticas útiles de los dispositivos y actividades detectadas.

Un software de monitoreo de la red es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red. La monitorización de redes también ayuda a optimizar la red, ya que facilita información detallada sobre el uso de la banda ancha y otros recursos de la red.

- AWSTATS:
    - Es una herramienta libre disponible bajo la licencia pública general GNU.
    - Trabaja tanto sobre plataforma Microsoft Windows como en Linux. En ambos casos se necesita que tenga instalado previamente el Perl.
    - Genera diversos tipos de cuadros estadísticos y gráficos que permiten analizar el uso de la red.
    - Origina reportes sobre el uso de determinadas aplicaciones tales como número de visitas al sitio web, procedencia de los usuarios de los servicios electrónicos, tipos de aplicaciones utilizadas, etc.
- Nagios:
    - Es un sistema de monitorización de redes de código abierto.

- Ofrece una monitorización completa y alerta para los servidores, *switchs*, aplicaciones y servicios.

- Detecta los problemas antes de que ocurran.

- Ayuda a reducir el tiempo de inactividad y pérdidas de la organización.

- Detecta fallos de seguridad.

- Proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas que pueden ser recibidas por los responsables correspondientes mediante correo electrónico y mensajes SMS.

1.2.2.2.8. Software de base de datos

Este software es el que provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.

El sistema de gestión de bases de datos (SGBD) es un conjunto de programas que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos. Los usuarios pueden acceder a la información usando herramientas específicas de interrogación y de generación de informes, o bien mediante aplicaciones al efecto.

El sistema de gestión de bases de datos proporciona métodos para mantener la integridad de los datos, administrar el acceso de usuarios a los datos y recuperar la información si el sistema se corrompe. Permite presentar la información de la base de datos en variados formatos. La mayoría de base de datos incluye un generador de informes. Los sistemas de gestión de bases de datos se encuentran en el corazón de toda aplicación que maneje datos. Se basan en sistemas operativos estándar para efectuar dichas funciones.

El sistema de gestión de bases de datos debe incluir un control de concurrencia, que permita a varios usuarios tener acceso simultáneo a dicha base de datos. Controlar la concurrencia implica que si varios usuarios acceden a la base de datos, la actualización de los mismos se haga de forma controlada para que no se presenten problemas con la información.

Los sistemas de base de datos relacionales son aquellos que almacenan y administran de manera lógica los datos en forma de tablas. Una tabla es a su vez un método para presentar los datos en la forma de filas y columnas. Cada columna representa un campo único de un registro. Varias de estas columnas o campo componen un registro, proveyendo información significativa e interrelacionada. Cada registro es representado en una fila. Al administrar las tablas y sus relaciones, aparecen los medios para insertar, borrar, consultar y actualizar la información de un sistema.

El software de base de datos debe proporcionar un potente mecanismo de seguridad que garantice que ningún intruso pueda acceder o corromper la integridad del sistema; la seguridad se puede clasificar a nivel de acceso al sistema, de objetos de datos, de datos, y seguridad en cuanto a protección de los almacenamientos físicos de los mismos.

- Microsoft SQL Server:

    - Es un sistema comercial que trabaja sobre plataforma Microsoft Windows.

    - Posee una gran variedad de herramientas administrativas y de desarrollo que permiten mejorar la capacidad de instalar, distribuir, administrar y utilizar.

    - Cuenta con el soporte técnico de Microsoft Corporation.

    - Se integra con el correo electrónico, internet y Windows, permitiendo una comunicación local.

    - Permite trabajar en modo cliente-servidor, donde la información y datos se alojan en el servidor y los terminales o clientes de la red acceden a la información.

    - Almacenamiento de datos.

    - Puede utilizarse el mismo motor de base de datos a través de plataformas que van desde equipos portátiles hasta grandes servidores con varios procesadores.

    - Provee escalabilidad, estabilidad y seguridad.

- MySQL:

    - Tiempo de respuesta rápida.

- Administración por consola o por herramientas gráficas.
- Es seguro.
- Reducción curva de aprendizaje.
- Maneja grandes bases de datos.
- Cuenta con varios programas cliente y bibliotecas.
- Cuenta con varias herramientas gráficas administrativas.
- Cuenta con una gran variedad de interfaces de programación.
- Licencia GPL.
- Mejor integración con PHP.
- No hay límite en el tamaño de los registros.
- Consume muy pocos recursos, tanto de CPU como de memoria.
- Seguridad altamente configurable.
- Trabaja tanto sobre plataforma Microsoft Windows como en Linux.

- PostgreSQL:

  - No necesita de licencias de software.
  - Es estable, es decir no es susceptible a caídas.
  - Se puede personalizar.
  - Trabaja tanto sobre plataforma Microsoft Windows como en Linux.
  - Entre sus características están la potencia y flexibilidad.
  - Por su arquitectura de diseño se necesita aumentar el número de CPU y la cantidad de memoria RAM.
  - Consume una gran cantidad de recursos.
  - Fue diseñado para ambientes de alto volumen.
  - Permiten la duplicación de bases de datos en múltiples sitios de réplica.
  - Cuenta con funciones de compatibilidad para ayudar en la transición desde otros sistemas menos compatibles con SQL.

1.2.3. Telecomunicaciones

Es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones.

1.2.3.1. Servicio de internet

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Internet es una red informática de transmisión de datos para la comunicación global que permite el intercambio de todo tipo de información (en formato digital) entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas *International Network* (red internacional).

Internet también se le conoce como red de redes o la gran red, debido a que su origen y filosofía se basan en interconectar computadores y ordenadores entre sí, creando una gran telaraña de intercomunicación, dichas interconexiones se realizan mediante línea telefónica, cable físico, redes inalámbricas, fibra óptica, vía satélite, telefonía móvil y tecnología PLC (*power line communications*).

- World Wide Web (www):

    - Uno de los servicios que más éxito ha tenido en internet.

- Es un sistema de comunicación o distribución de información basada en hipertexto o hipermedios enlazados y accesibles a través de internet.

- Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces.

- El funcionamiento de la web ocurre mediante navegadores web ejemplos: Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Netscape Navigator y Safari. El usuario puede visualizar el contenido incluido en páginas y sitios web a través de direcciones URL.

- Tele Network (Telnet):

  - Es un programa que permite acceder a ordenadores distantes en internet a través de credenciales.

  - Una vez que se ha accedido a un sistema distante, se pueden descargar ficheros y realizar las mismas funciones que si se estuviese directamente conectado al ordenador distante.

  - Se necesita tener una cuenta de internet para poder utilizar el telnet.

  - No hay una interfaz gráfica, es a través de modo terminal.

  - Se dejó de usar casi por completo por tener problemas de seguridad (no encripta la información).

- Protocolo de transferencia de archivos (FTP):

    - Es un software cliente/servidor que permite a usuarios transferir ficheros entre ordenadores en una red TCP/IP.

    - Es el sistema de transferir archivos más estable y fiable que hay en internet. Esto significa que la descarga y subida de archivos que se realicen tendrán más opciones de completarse sin errores de transferencia, y quedarán intactos después del envío.

    - Algunos clientes de FTP básicos en modo consola vienen integrados en los sistemas operativos, incluyendo Microsoft Windows, DOS, GNU/Linux y Unix. Sin embargo, hay disponibles clientes con opciones añadidas e interfaz gráfica. Aunque muchos navegadores tienen ya integrado FTP, es más confiable a la hora de conectarse con servidores FTP no anónimos utilizar un programa cliente.

    - Existen muchos clientes FTP, entre estos se encuentran: FileZilla, CuteFtp, WS Ftp, Coffe Cup, CoreFtp, WorldWide Ftp y Ftp Now.

- Correo electrónico (POP y SMTP):

    - Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos.

- Principalmente se usa este nombre para denominar al sistema que provee este servicio en internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías.

- Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales, dependiendo del sistema que se use.

- Su eficiencia, conveniencia y bajo costo están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

- El correo electrónico es una de las funcionalidades más utilizadas de internet, ya que contribuye a comunicaciones veloces, confiables y precisas.

- Uno de los grandes problemas con que se ha topado esta tecnología es la cantidad de spam o correo basura que es enviado y recibido por día.

- Peer-to-peer (P2P):

  - Es una red descentralizada que no tiene clientes ni servidores fijos, sino que una serie de nodos que se comportan simultáneamente como clientes y servidores de los demás nodos de la red. No existe una autoridad central única que se pueda eliminar o bloquear y colapsar toda la red.

- La ventaja principal de la tecnología P2P es que saca el máximo partido de los recursos (ancho de banda, capacidad de almacenamiento, etc.) de los muchos clientes/peers para ofrecer servicios de aplicación y red, sin tener que confiar en los recursos de uno o más servidores centrales. Entre más nodos se incorporen a la red de más recursos se disponen, ya que estos son compartidos entre ellos.

- Su función es el intercambio de archivos de cualquier tipo, como audio, vídeo, texto o software, entre los usuarios de la red.

- Mensajería instantánea (IM):

  - Es una forma de comunicación en tiempo real entre dos o más personas, basada en texto. El texto es enviado a través de dispositivos conectados a una red como internet.

  - Para la mensajería instantánea se emplea un cliente (programa mensajero) que suele mostrar los usuarios conectados y su estado de disponibilidad (de una lista de usuarios que previamente agregó el propietario de la cuenta de mensajería, la lista de contactos). A los usuarios conectados se les pueden enviar mensajes de texto, y en algunos mensajeros, también gráficos, sonidos, animaciones, archivos, videos y webcam. Algunos permiten compartir recursos y juegos entre usuarios, y también asociar la cuenta del mensajero a otros servicios como weblogs y servicio de emails.

  - Actualmente existen en el mercado servicios como Whats App, BlackBerry Messenger, Google Hangouts, Skype, Line, Viber, Yahoo!

Messenger, AOL Instant Messenger, NET Messenger o algunos especialmente trabajados para las empresas, como Confide.

- Algunas organizaciones usan este servicio como parte de sus herramientas de productividad y comunicación. Por otro lado, también existen empresas que prohíben el uso de mensajería instantánea por considerarlo una distracción a los empleados.

1.2.3.2. Router

El *router* es el dispositivo que permite administrar el tráfico de datos entre la red local y el internet; se encarga de garantizar que las comunicaciones lleguen al destinatario correcto. Además, puede realizar algunas tareas de seguridad de las comunicaciones.

El *router* toma decisiones con base en diversos parámetros con respecto de la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.

El *router* trabaja a nivel de red (capa tres o capa de red) del modelo OSI, por tanto utiliza direcciones IP. Habitualmente se utilizan para conectar una red de área local a una red de área extensa. Es capaz de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo.

1.2.3.3. Línea telefónica

Es un circuito de un sistema de comunicaciones por teléfono. Típicamente, se refiere a un cable físico u otro medio de transmisión de señales que conecte el aparato telefónico del usuario a la red de telecomunicaciones, y normalmente

supone también un único número de teléfono asociado a dicho usuario para poder facturarle el servicio prestado.

Las frecuencias presentes en la voz van desde: 100 Hz hasta 6 kHz; la mayor parte de la energía necesaria para hacer inteligible un diálogo está entre: 200 Hz hasta 4 kHz; la reducción del ancho de banda (300 - 3300 Hz.) es para eliminar ruido. La banda de paso de un sistema telefónico se conoce como VF (*Voice Frequency Channel*) 4 kHz.

Los cables de la telefonía son normalmente de cobre (aunque también se ha usado aluminio) y se llevan de dos en dos, separados aproximadamente 25 cm, sobre postes, y más tarde como pares trenzados. Las líneas modernas pueden ir bajo tierra a un conversor analógico-digital que convierte la señal analógica a digital para transmitirla por fibra óptica. La mayoría de los hogares están conectados mediante conductores RJ11 de cobre.

1.2.4. Red de área local

Una red informática consiste en dos o más ordenadores conectados entre sí para poder compartir recursos, tales como impresoras, *scanner*, ficheros etc.

1.2.4.1. Cableado de red

Los cables de red son elaborados para transmitir datos y se usan para interconectar un dispositivo de red a otro. Estos habilitan transferencias de alta velocidad entre diferentes componentes de la red.

Los tipos de cable de red son variados dependiendo de la clase de red donde se usen. Se utilizarán distintos cables con base en la topología de la red, protocolos en uso y tamaño. Si la red tiene un gran número de dispositivos, necesitará cables que provean de alta velocidad y conexiones libres de errores.

Algunos de los cables que se usan hoy en día son los cables UTP (*unshielded twisted pair*), cables coaxiales y fibra óptica.

Los cables UTP o de par trenzado, son la variedad más popular, muy usada en todo tipo de redes con velocidades de hasta 100 Mbps (en categoría de 6 hasta 1000 Mbps).

Los cables coaxiales tienen un único conductor en el centro normalmente llamado “alma” o “activo”. Una capa de plástico rodea este conductor central y lo aísla a su vez de la malla metálica que corresponde a la masa.

Los cables de fibra óptica consisten en un núcleo de vidrio rodeado por capas de materiales protectores. Transmite señales de luz en contraposición de señales electrónicas y las envía a distancias mucho más largas que los cables coaxiales y de pares.

Una red de área local (LAN) requiere cables de red para realizar sus conexiones. Se pueden entender los cables de red como el esqueleto de la red. Sin embargo, las redes cada vez utilizan más otros medios para transferir datos, tales como señales de radio (WIFI), para conexionar las estaciones de trabajo.

1.2.4.2. *Switch* Ethernet

Es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

El *switch Ethernet* se utiliza cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

El *switch* toma decisiones con base en las direcciones MAC y por lo tanto, son dispositivos de la capa 2. Dado que un *switch* tiene la capacidad de tomar decisiones de selección de la ruta, la red se vuelve mucho más eficiente.

El *switch* aprende qué *hosts* están conectados a un puerto leyendo la dirección MAC origen en las tramas. El *switch* abre un circuito virtual solo entre los nodos origen y destino. Esto limita la comunicación a estos dos puertos sin afectar el tráfico en otros puertos.

1.2.5. Herramientas de administración de servicios

A continuación se presentan herramientas que son fundamentales dentro de la organización para poder alcanzar sus objetivos.

1.2.5.1. Software

- Sistema operativo Microsoft o Linux:
  - En sus diferentes versiones para computadoras personales, Microsoft Windows es el sistema operativo comercial más ampliamente usado.

- Sistema antivirus:

  - ESET NOD32 es un sistema antivirus comercial que trabaja sobre plataforma Microsoft Windows.

  - Avast! Linux home Edition es un sistema antivirus para Linux que se ofrece con licencia libre para uso no comercial.

- Software cliente de correo electrónico:

  - Outlook Express de Microsoft Windows es el programa que viene incluido en el Microsoft Internet Explorer a partir de la versión 4.

  - Zimbra es la solución libre para correo electrónico y calendario de código abierto.

- Software para diseño gráfico:

  - GIMP (GNU, *Image Manipulation Program*) es una aplicación libre de costo orientada a la manipulación de imágenes. Trabaja sobre las plataformas Microsoft Windows y Linux.

- Photoshop de Adobe es el producto comercial manejador de gráficos más popular y cuenta con el mayor surtido de funciones gráficas.

- Software para edición de páginas web:

  - KompoZer es un editor web gratuito para lenguaje HTML basado en el popular NVU (editor WYSIWYG multiplataforma construido sobre Mozilla Composer). Permite a usuarios sin conocimiento alguno de programación crear su propia página web partiendo desde cero, mediante la simple introducción de diversos elementos (botones, imágenes, tablas, formulario, etc.) en el entorno de la página web.

  - Dreamweaver es un editor comercial de Adobe disponible para Windows. Ofrece más funciones para la creación, edición y publicación de páginas web.

- Software de edición de documentos MS Office u Open Office:

  - MS Office es una suite de oficina que abarca e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows y Mac OS X.

  - OpenOffice es una suite ofimática libre (código abierto y distribución gratuita) que incluye herramientas como procesador de textos, hoja de cálculo, presentaciones, herramientas para el dibujo vectorial y base de datos.

1.2.5.2. Hardware

- Computadora:

    - Es una máquina electrónica que permite procesar y acumular datos para convertirlos en información útil. Es un equipo indispensable en la vida cotidiana, que también se conoce por el nombre de computador u ordenador.

    - En la computadora se pueden realizar tareas muy diversas, cargando distintos programas en la memoria para que los ejecute el procesador.

    - La estructura básica de una computadora incluye microprocesador (CPU), memoria y dispositivos de entrada/salida (E/S), junto a los buses que permiten la comunicación entre ellos.

- Impresora:

    - Es un equipo cuya finalidad es la de reproducir en papel los textos o gráficos de los diversos documentos almacenados en formato electrónico. Principalmente se busca calidad y rapidez en el proceso de impresión.

    - Existen varios tipos de impresoras, incluyendo las LED, láser, térmica, de inyección de tinta y de matriz de puntos.

- Escáner:

    - Es un equipo diseñado para capturar en forma óptica las imágenes o textos de documentos y llevarlos a un formato digital para ser procesados en una computadora.

    - Los escáneres no distinguen el texto de los gráficos, por lo tanto, debe existir un procesamiento de la imagen escaneada para generar texto editable. Este proceso es llamado OCR, y existen múltiples aplicaciones para tal fin.

    - Actualmente los escáneres vienen junto con las impresoras; estos dispositivos son llamados impresoras multifunción.

- Fotocopiadora:

    - Una fotocopiadora es aquella máquina que se utiliza para copiar algún documento, es decir, para fabricar copias de papel a papel.

    - El tamaño de los papeles es muy variado: carta, oficio, A4, A5, y muchos más hasta llegar a los especiales para planos.

    - Actualmente hay fotocopiadoras de tamaños y funciones variadas; hay personales, de escritorio, de estación, de planos, etc. Algunas se pueden conectar en red, otras son multifuncionales (que son también escáner, fax, impresora, etc.).

1.3. Regulación de los recurso tecnológicos

Regulación es la acción y efecto de regular (ajustar o poner en orden algo, reglar el funcionamiento de un sistema, determinar normas). El término suele utilizarse como sinónimo de normativa.

La regulación, por lo tanto, consiste en el establecimiento de normas, reglas o leyes dentro de un determinado ámbito. El objetivo de la regulación es mantener un orden, llevar un control y garantizar los derechos de todos los integrantes de una comunidad.

En la actualidad la sociedad se mueve a una velocidad impresionante. Los cambios tecnológicos ocurren tan rápido que no se ha terminado la asimilación de la última tecnología y ya aparece otra. Los mercados se tornan muy competitivos y para poder insertarse en ellos es necesaria la innovación constante como la única estrategia de supervivencia, para la organización.

El progreso y desarrollo de una organización depende directamente de su capacidad para adaptarse con rapidez a los cambios del entorno, en especial del entorno tecnológico, e incluso para provocar modificaciones que les favorezcan.

Uno de los principales retos que debe asumir toda organización es regular la utilización de los medios y recursos tecnológicos puestos a disposición de los trabajadores.

La relación entre la organización y el trabajador debe ser fluida; es necesario que la regulación de los medios de producción se efectúe de forma clara estableciendo los límites y medios.

Los recursos tecnológicos puestos a disposición de los empleados de la organización deben garantizar la seguridad, disponibilidad, fiabilidad y privacidad de las comunicaciones, así como también preservar la privacidad de los empleados.

El empleado debe ser consciente que es responsable de no abusar en la utilización de los recursos tecnológicos puestos a su disposición, manteniendo el respeto a los derechos de los demás usuarios, y cumpliendo con las normas que la empresa le definió; entre los aspectos que debería contener una política que regule los usos de los recursos tecnológicos de la organización se podrían destacar:

- Asignación de claves y la política de contraseñas, debiendo definirse los procedimientos para la asignación, distribución, confidencialidad y configuración de las contraseñas de acceso, la cual es de carácter individual y privada.

- Utilización del correo electrónico, debiendo definirse el uso del correo personal dentro del horario de trabajo, así como el uso del correo de la empresa como medio de distribución de información y las limitaciones de su uso.

- Restricciones a la navegación por internet, definiendo la utilización de la red para navegar por sitios *web*, para otros usos que no sean los permitidos en el desempeño de su actividad.

- Prohibición del uso de herramientas y redes P2P, debiendo definir la prohibición clara de instalar herramientas no autorizadas y el acceso a

redes de intercambio de archivos o programas propiedad de la organización.

- Uso de equipos informáticos fuera de la empresa, definiendo cuáles serán los dispositivos y la información que puede salir fuera de la organización, precisando la seguridad que debe conferirse a los equipos.

- Restricciones en el uso de mensajería instantánea, como medio de comunicación externa a la actividad empresarial.

- Restricción en la divulgación de información reservada de la organización a otras personas, si no se está autorizado para ello.

- Restricción en los recursos informáticos de la organización podrán usarse para fines diferentes a los del puesto de trabajo; por ejemplo las impresiones que se elaboren con este recurso no pueden ser de carácter personal.

Las organizaciones deberían disponer de herramientas de control que les permitan analizar y detectar los usos y comportamientos indebidos o ilícitos en los recursos, los cuales puedan suponer un riesgo en la seguridad de los sistemas de la empresa.

Resulta fundamental establecer previamente las reglas de uso de los recursos tecnológicos con aplicación de prohibiciones absolutas o parciales e informar a los empleados de la existencia de controles.

La utilización de los medios y recursos tecnológicos propiedad de la organización por el trabajador, implica atender a distintas normativas de

ámbitos muy diferentes que conllevan la imperiosa necesidad de trasladar a los empleados políticas en el uso de los medios de producción, que garanticen la seguridad de la información y utilizando herramientas de control por parte de la empresa, que le permitan analizar y detectar los usos y comportamientos indebidos o ilícitos de los recursos, quedando claro que la regulación de los recursos tecnológicos de forma correcta no trasgrede el ámbito privado del empleado.

2. RIESGO INFORMÁTICO

2.1. Definición de riesgo

El riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan se convierten en un riesgo, o sea en la probabilidad de que ocurra un desastre.

El riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado, un riesgo conlleva dos tipos de consecuencias: ganancias o pérdidas.

Cuando en un proceso existe la posibilidad de que haya una alteración respecto de los resultados, se debe entender que existe un riesgo. Así, el riesgo se puede entender como la variación que se puede producir en los resultados esperados de una situación dada, dentro de un período determinado.

Un riesgo tiene potencial para dañar a las personas, aún aquellas que tienen experiencia y conocimiento sobre su trabajo, dañar a la propiedad, afectar significativamente la cantidad, calidad y/o los costos de producción, los indicadores de productividad.

El riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia.

El riesgo a nivel de tecnología, se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida; por ejemplo el riesgo de perder datos debido a rotura de disco o un virus informático.

Cada organización tiene una misión. En esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben estar conscientes de que la administración del riesgo informático juega un rol crítico.

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, finanzas, entre otro; y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio; es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

Los sistemas de información son vulnerables a una diversidad de amenazas y atentados por parte de personas tanto internas como externas de la organización:

- Desastres naturales, por servicios, suministros y trabajos no confiables e imperfectos, por la incompetencia y las deficiencias cotidianas, por el abuso en el manejo de los sistemas informáticos, por el desastre a causa

de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputo.

2.1.1. Probabilidad

La probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, debe considerarse en cada caso que es posible que la amenaza se presente, independientemente del hecho que sea o no contrarrestada.

Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (series históricas, compañías de seguros y otros datos) para establecer con razonable objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; se hacen estimaciones sobre la base de experiencias.

La probabilidad de que una vez presentada la situación de riesgo, se origine el accidente. Habrá que tener en cuenta la secuencia completa de acontecimientos que desencadenan el accidente.

La probabilidad de que ocurra el daño se puede graduar, desde baja hasta alta, con los siguientes criterios:

- Probabilidad alta: el daño ocurrirá siempre o casi siempre
- Probabilidad media: el daño ocurrirá en algunas ocasiones
- Probabilidad baja: el daño ocurrirá raras veces

La evaluación de la probabilidad requiere formarse una opinión sobre un evento futuro o sobre un conjunto de circunstancias que no han ocurrido todavía. Personas diferentes tendrán visiones diferentes del futuro, y no hay una única respuesta correcta, puesto que el futuro no ha ocurrido todavía.

La evaluación de probabilidad incorrecta significa que los riesgos serán priorizados de forma equivocada, conllevando al fallo para centrarse en los riesgos más significativos, selección de respuestas inapropiadas, inhabilidad para gestionar los riesgos de forma efectiva, y pérdida de confianza en el proceso de riesgos.

La evaluación de la probabilidad de riesgo acertada mejora el entendimiento de cada riesgo, permitiendo la priorización adecuada, mejor selección de la respuesta, mejor efectividad en la gestión del riesgo, y un alcance más fiable de los objetivos del proyecto y del negocio.

Es necesario entender los problemas asociados con la evaluación de probabilidad, y llevar a cabo alguna acción para direccionarlos, utilizando el lenguaje y los formatos apropiados, identificando y gestionando los recursos predispuestos, lecciones aprendidas, la efectividad del proceso de evaluación de la probabilidad, y monitoreando el desempeño de la gestión del riesgo para determinar la exactitud de la probabilidad de riesgo evaluada.

2.1.2. Amenazas

Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, los ingresos no autorizados, los virus, uso inadecuado de software, los desastres ambientales

como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño material o inmaterial sobre los elementos de un sistema.

Las amenazas pueden ser de carácter físico o lógico, como una inundación o un acceso no autorizado a una base de datos.

Un alto porcentaje de ataques informáticos se realizan con la intención de obtener ganancias financieras para el atacante, por ejemplo el hackeo de páginas de instituciones financieras con el fin de lograr hacer transferencias de dinero, o bien robar información confidencial de diversas organizaciones que posteriormente pueda ser vendida a terceros.

Existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

La presencia de una amenaza es una advertencia de que puede ser inminente el daño a algún activo de la información, o bien es un indicador de que el daño se está produciendo o ya se ha producido.

2.1.3. Vulnerabilidades

La vulnerabilidad se refiere a ciertas condiciones inherentes a los activos o presentes en su entorno que facilitan que las amenazas se materialicen; llevan a esos activos a ser vulnerables. Mediante el uso de las debilidades existentes es que las amenazas logran materializarse; las amenazas siempre están presentes, pero sin la identificación de la vulnerabilidad no podrán ocasionar ningún impacto.

Las vulnerabilidades son de naturaleza variada. Por ejemplo, la falta de conocimiento del usuario, tecnología inadecuadamente probada, transmisión por redes públicas, entre otros.

La vulnerabilidad hace referencia a una debilidad en un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado, la amenaza de virus, si bien potencialmente sigue, no podría materializarse.

Las vulnerabilidades son fallos en el software informático que crean debilidades en la seguridad global de la computadora o de la red. Las vulnerabilidades también pueden producirse por configuraciones inadecuadas del computador o de la seguridad. Los piratas informáticos explotan estas debilidades, causando daños al computador o a la información.

Las vulnerabilidades más peligrosas son aquellas que le permiten a un atacante ejecutar código arbitrario, lo que le brindaría la oportunidad de tomar el control de la computadora, sometiéndola a sus requerimientos. A continuación se listan vulnerabilidades de los sistemas informáticos:

- Debilidad en el diseño de los protocolos utilizados en las redes. Ej. Telnet, FTP, SNMP (*simple network management protocol*) también conocido como *security not my problem*, errores de programación, configuración inadecuada de sistemas informáticos, políticas de seguridad deficiente o inexistente, desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, disponibilidad de herramientas que facilitan los ataques. Entre los equipos que son vulnerables se encuentran: *routers*, módems, cámaras web, servidores de video, impresoras, escáneres, faxes, fotocopiadoras, teléfonos móviles (*snarfing* o *bluesnarfing*).

  Los software o aplicaciones que son vulnerables son: sistemas operativos, bases de datos, navegadores, aplicaciones de oficina (Word, Excel, etc.), utilerías (winamp, wmp, *flash*, etc.).

En la revisión de equipos y servidores se deberían analizar y evaluar los siguientes aspectos:

- Parches del sistema operativo, seguridad en los archivos, cuentas de usuarios, servicios y aplicaciones instaladas, protocolos y servicios de red, control de acceso a los recursos, registro y auditoría de eventos, configuración de las herramientas de seguridad: antivirus, cortafuegos (*firewall*), copias de seguridad, pruebas de penetraciones internas y externas.

Las organizaciones son cada vez más dependientes de sus sistemas y servicios de información, por lo tanto son cada vez más vulnerables a las amenazas concernientes a su seguridad.

2.1.4. Activos

El activo es un objeto o recurso de valor empleado en una empresa u organización. Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplo los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.

Los activos son vulnerables hacia una amenaza si no se protegen adecuadamente, poniendo en peligro la confidencialidad, integridad o disponibilidad de ese activo, causando daños o perjuicios a la organización.

Los activos de la organización se pueden clasificar de la siguiente forma:

- Software:
  - Aplicaciones comerciales, aplicaciones de gestión y base de datos.

- Hardware:
  - Servidores, terminales de trabajo, red de comunicaciones interna y red de comunicaciones remota.

- Infraestructura:
  - Oficinas.

- Personal:
  - Personal subcontratado y empleados.

- Datos:
    - Expedientes, contabilidad e información.

El valor de un activo depende de varios factores:

- Costo de adquisición, información contenida, procesos controlados e impacto en la organización cuando falle.

2.1.5. Impactos

El impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza.

Las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

Se puede establecer que los impactos más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio. Otras no tan comunes, felizmente, se refiere a la pérdida de vidas humanas, afectación del medio ambiente, etc.

El impacto que produce la amenaza en la organización no depende de las características de la vulnerabilidad, sino del grado de criticidad de la parte del sistema informático en que puede llegar a actuar.

En relación con el impacto de un ataque exitoso, sus consecuencias pueden ser múltiples, a veces son imprevisibles y dependen mucho del contexto donde se maneje la información, sea en una ONG (derechos humanos, centro

de información entre otro.), en una empresa privada (banco, clínica, producción etc.), en una institución estatal o en el ámbito privado.

Para una correcta valoración del impacto es aconsejable tener en cuenta tanto los daños tangibles como los intangibles, incluida la información. Para ello es necesario reunirse con los responsables de departamentos y evaluar el grado de impacto que podría tener en su ámbito de trabajo.

El impacto causado por la materialización de las amenazas se valora en términos subjetivos (impacto muy alto, alto, medio, bajo o muy bajo). Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento y de competitividad, interrupción de negocio, pérdida de imagen, entre otro.).

2.2. Administración y análisis de riesgo

El análisis de riesgos corresponde al estudio de los eventos que tienen efectos sobre la actividad de la organización.

El análisis de riesgo es la consideración sistemática del daño probable que puede causar en la organización un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

El análisis de riesgos permite determinar cómo es, cuánto vale y qué tan protegidos se encuentran los activos de la organización.

El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento; determina los componentes de un sistema que requiere protección, las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

El análisis de riesgo tiene como objetivo identificar los riesgos mediante el reconocimiento de sus elementos y lograr establecer el riesgo total o exposición bruta al riesgo y luego el riesgo residual, ya sea en términos cuantitativos o cualitativos.

El análisis de riesgos es una técnica utilizada para determinar el riesgo, siguiendo los pasos establecidos:

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio a nivel de costo supondría su degradación.

- Determinar a qué amenazas están expuestos aquellos activos.

- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

Los resultados del análisis de riesgos, una vez realizado, permiten que la organización tenga en sus manos una poderosa herramienta para el tratamiento de sus vulnerabilidades y un diagnóstico general sobre el estado de la seguridad de su entorno como un todo.

A continuación se mencionan algunas metodologías de análisis de riesgo usadas:

- Magerit:

    - Metodología de análisis y gestión de riesgos de los sistemas de información: fue desarrollada por el Ministerio de Administraciones Públicas de Madrid; está enfocada a la información mecanizada y a los sistemas informáticos que la tratan; dicha metodología permitirá saber cuántos de los activos de la empresa están en juego y cómo protegerlos.

    - Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información; esto supone beneficios para los usuarios y da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

    - Magerit implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones, teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

- Magerit persigue concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Magerit ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

- MECI:

  - Modelo estándar de control interno para el estado colombiano; proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, y aunque promueve una estructura uniforme, se adapta a las necesidades específicas de cada empresa, a sus objetivos, estructura, tamaño, procesos y servicios que suministran.

  - MECI proporciona una estructura para el control a la estrategia, la gestión y la evaluación en las entidades del Estado, cuyo propósito es orientarlas hacia el cumplimiento de sus objetivos institucionales y la contribución de estos a los fines esenciales del Estado.

  - Establece las políticas, métodos y mecanismos de prevención, control, evaluación y de mejoramiento permanente de la entidad pública, que le permiten el cumplimiento de sus objetivos institucionales y la finalidad social del Estado en su conjunto.

  - Se fundamenta en la construcción de una ética institucional, orientada a la prevención del riesgo. Se hace efectivo en una organización por procesos (gestión de calidad), encausa la entidad a

un control corporativo permanente, mide la gestión en tiempo real, genera información de utilidad organizacional y social, fortalece la evaluación independiente, estandariza de procedimientos y otorga nivel de importancia a los planes de mejoramiento institucional.

- OCTAVE:

  - Es una metodología de análisis de riesgos desarrollada por la Universidad Carnegie Mellon en el 2001, y su acrónimo significa “Operationally Critical Threat, Asset and Vulnerability Evaluation“; estudia los riesgos con base en tres principios: confidencialidad, integridad y disponibilidad; esta metodología se emplea por distintas agencias gubernamentales, tales como el departamento de defensa de Estados Unidos.

  - Es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo.

  - Establece un equilibrio entre tres aspectos: riesgo operacional, tecnología y prácticas de seguridad.

  - Permite a las organizaciones entender, valorar y hacer frente a sus riesgos de seguridad de la información desde la perspectiva de la organización.

  - Los activos (las personas, el hardware, la información, los sistemas) son ordenados de acuerdo con la importancia de los objetivos estratégicos de la organización, las posibles amenazas y

vulnerabilidades que pueden presentarse en cada uno de ellos y el impacto de dicha amenaza con relación con la empresa.

El análisis de riesgos a partir de los resultados permite hacer recomendaciones de seguridad, para que la organización pueda evaluar los riesgos a que está sometida y conocer cuáles son los activos de los procesos de negocio que están más susceptibles a la acción de amenazas, a la confidencialidad, integridad y disponibilidad de la información utilizada, para alcanzar los objetivos intermedios o finales de la organización.

La dinámica en la cual se ven inmersas las organizaciones actualmente demanda un esfuerzo que ante cada nuevo emprendimiento debe realizarse en tempranas etapas un análisis de riesgo del referido proyecto, así como su impacto en la estructura de riesgos de la organización.

La administración de riesgo es planear, organizar, dirigir y ejecutar tanto procesos como actividades conducentes, para asegurar que la organización esté protegida apropiadamente contra los riesgos que podrían afectarla.

La administración de riesgo es el proceso por el cual la dirección de una empresa u organización administra el amplio espectro de los riesgos a los cuales está expuesta, tanto sean de mercado como operacionales, de acuerdo con el nivel de riesgo al cual están dispuestos a exponerse, según sus objetivos estratégicos.

La administración de riesgos es la aplicación de estrategias para evitar o reducir los costos generados por los riesgos.

Administrar el riesgo refiere a gestionar los recursos de la organización para lograr un nivel de exposición determinado.

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de varios pasos, los cuales, cuando son ejecutados de manera secuencial, posibilitan una mejora continua en el proceso de toma de decisiones.

El ciclo de administración de riesgo se cierra luego de efectuar las tareas referentes al análisis con la determinación de las acciones a seguir respecto de los riesgos residuales identificados. Las acciones de administración pueden ser:

- Controlar el riesgo: se fortalecen los controles existentes o se agregan nuevos.

- Eliminar el riesgo: se elimina el activo relacionado y por ende el riesgo.

- Compartir el riesgo: mediante acuerdos contractuales se traspasa parte del riesgo o su totalidad a un tercero.

- Aceptar el riesgo: determinar que el nivel de exposición es adecuado.

2.3. Proceso de administración del riesgo

La administración de riesgos es un proceso continuo, dado que es necesario evaluar periódicamente si los riesgos identificados y la exposición a los mismos se mantienen vigentes.

Entre los elementos principales del proceso de administración de riesgos, se pueden mencionar:

- Comunicar y consultar

    - Comunicar y consultar con interesados internos y externos según resulte apropiado en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

    - Es útil un enfoque de equipo de consulta para ayudar a definir el contexto en forma apropiada, para ayudar a que los riesgos sean identificados eficazmente, para reunir distintas áreas de especialidad en el análisis de riesgos y asegurar que se consideran distintos puntos de vista en la evaluación de los mismos, para una administración apropiada de cambios durante su tratamiento.

    - Es importante desarrollar un plan de comunicación tanto para los interesados internos como externos en la etapa más temprana del proceso. Este plan debería considerar aspectos relativos tanto al riesgo en sí mismo, como al proceso para administrarlo.

    - Las percepciones sobre el riesgo pueden variar debido a diferencias en los valores, necesidades, suposiciones, conceptos y preocupaciones en los interesados, en la medida que se relacionen con el riesgo o los aspectos bajo discusión.

    - La comunicación interna y externa es importante para asegurar con los responsables la implementación de administración de riesgo, y los que tiene un interés establecido, comprendan la base sobre la

cual se toman las decisiones y por qué se requieren determinadas acciones.

- Establecer el contexto

  - Establecer los contextos estratégicos, organizacionales y de administración de riesgos en los cuales tendrá lugar el resto de los procesos. Deberán establecerse los criterios contra los cuales se evaluarán los riesgos y definir la estructura del análisis.

  - Antes de comenzar una actividad de administración de riesgos, a cualquier nivel, es necesario comprender la organización, su estructura y sus capacidades, como también sus metas, objetivos y las estrategias que están vigentes para lograrlos.

  - El riesgo principal para la mayoría de las organizaciones es fallar en el logro de sus objetivos estratégicos, de negocio o de proyectos, o que sean percibidos como fallados por los interesados.

  - Definir la relación entre la organización y el entorno externo, social y político, identificando las fortalezas, debilidades, oportunidades y amenazas de la organización. El contexto incluye los aspectos financieros, operacionales, competitivos y políticos, percepción e imagen pública, social, clientes, cultural y legal de las funciones de la organización.

  - Deben establecerse las metas, objetivos, estrategias, alcances y parámetros de la actividad, o parte de la organización a la cual se está aplicando el proceso de administración de riesgos.

- El proceso debería ser llevado a cabo con plena consideración a la necesidad de balancear costos, beneficios y oportunidades, especificando los recursos requeridos y los registros a mantener.

- Los criterios de riesgo son inicialmente desarrollados como parte del establecimiento del contexto de administración de riesgos, los mismos deben ser posteriormente refinados a medida que se identifiquen los riesgos particulares y se escojan técnicas de análisis de riesgos.

- Identificar riesgos

  - Identificar qué, por qué, dónde, cuándo y cómo los eventos podrían impedir, degradar, demorar o mejorar el logro de los objetivos estratégicos y de negocio de la organización.

  - La identificación debería incluir todos los aspectos de los riesgos, estén o no bajo control de la organización.

  - El propósito es generar una lista amplia de fuentes de riesgos y eventos que podrían tener un impacto en el logro de cada uno de los objetivos estratégicos, de la organización o de proyecto. Estos eventos podrían impedir, degradar, demorar o mejorar el logro de esos objetivos.

  - Habiendo identificado lo que podría suceder, es necesario considerar las causas y escenarios posibles. Hay muchas causas en que puede suceder un evento. Es importante que no se omita ninguna causa significativa.

- Los enfoques utilizados para identificar riesgos incluyen lista de chequeo, juicios basados en experiencia y registros, diagramas de flujo, técnica de lluvias de ideas, análisis de sistemas y de escenario. El enfoque utilizado dependerá de la naturaleza de las actividades bajo revisión, de los tipos de riesgos y del contexto organizacional.

- Analizar riesgos

  - Determinar los controles existentes y analizar los riesgos en términos de consecuencia y probabilidad en el contexto de tales controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que esas consecuencias puedan ocurrir. Consecuencia y probabilidad puedan ser combinadas para producir un nivel estimado de riesgo.

  - El objetivo del análisis de riesgo es proveer un ingreso de datos a las decisiones sobre si los riesgos necesitan ser tratados y sobre las estrategias más apropiadas y costos eficaces de tratamiento de los riesgos.

  - El análisis de riesgos involucra considerar las fuentes de riesgo, sus consecuencias positivas y negativas y las probabilidades de que esas consecuencias puedan ocurrir. El riesgo es analizado combinando consecuencias y probabilidades, tomando en cuenta las medidas de control existentes.

  - Los riesgos excluidos deberían ser listados para demostrar la integridad del análisis de riesgo.

- El análisis de riesgo debería ser llevado a cabo a distintos niveles de detalle dependiendo del riesgo, y de la información, datos y recursos disponibles.

- Dado que algunas estimaciones realizadas en el análisis del riesgo son imprecisas, deberá llevarse a cabo un análisis de sensibilidad para verificar el efecto de la incertidumbre en las suposiciones y datos. El análisis de sensibilidad es también una forma de comprobar la adecuación y efectividad de los controles y de las opciones de tratamiento de riesgos potenciales.

- Evaluar riesgos

  - Comparar los niveles estimados de riesgo contra los criterios preestablecidos y considerar el balance entre beneficios potenciales y resultados adversos. Esto permite realizar apreciaciones sobre prioridades gerenciales.

  - El objetivo de la evaluación de riesgos es tomar decisiones, basadas en los resultados del análisis, acerca de los riesgos que requieren tratamiento y sus prioridades.

  - Los riesgos bajos o tolerables podrían ser aceptados con un tratamiento futuro mínimo. Los mismos deberían ser monitoreados y revisados periódicamente para asegurar que se mantengan igual.

- Tratar riesgos

  - Si los niveles de riesgo establecidos son bajos y son tolerantes no se requiere tratamiento. Para otros riesgos desarrollar e implementar estrategias y planes de acción específicos para aumentar los beneficios potenciales y reducir los costos potenciales.

  - El tratamiento del riesgo involucra identificar el rango de opciones para tratar el riesgo, evaluar esas opciones, preparar planes de tratamiento e implementarlos.

  - Las opciones de tratamiento de riesgos deben ser evaluadas sobre la base del grado de reducción de las pérdidas, y el alcance de cualquier beneficio adicional u oportunidades creadas. Puede considerarse y aplicarse una cantidad de opciones, ya sea individualmente o combinadas.

  - La selección de la opción más apropiada involucra balancear el costo de implementar dicha opción contra los beneficios derivados de la misma; el costo de administrar los riesgos necesita ser conmensurado con los beneficios obtenidos.

  - Las estrategias de tratamiento de riesgos podrían por sí mismas introducir nuevos riesgos. Estos riesgos necesitan ser identificados, evaluados, tratados y monitoreados como parte del proceso iterativo.

  - Los planes de tratamiento deben identificar las responsabilidades, fechas programadas, resultados esperados, presupuesto, y medidas del desempeño. Los planes deberían incluir mecanismos para

evaluar la implementación de las opciones respecto de criterios de desempeño, responsabilidades individuales y otros objetivos.

- Monitorear y revisar

  - Monitorear y revisar el desempeño de las estrategias de control de riesgo y procurar detectar cambios que pudieran afectar la adecuación o eficacia de costo de los controles.

  - Es necesario monitorear la eficacia de todos los pasos del proceso de administración de riesgos. Este es un paso importante para la mejora continua.

  - Los riesgos y la eficacia de las medidas de tratamiento necesitan ser monitoreados para asegurar que las circunstancias cambiantes no alteren las prioridades. La autoevaluación del control provee un medio para la revisión continua de los riesgos y sus controles.

  - Es esencial la revisión sobre la marcha para asegurar que el plan de administración se mantenga relevante. Los factores que podrían afectar la probabilidad y consecuencias de un resultado pueden cambiar. Es necesario repetir el ciclo de administración de riesgos regularmente.

  - El monitoreo también involucra aprender de los eventos y de sus resultados.

Es muy importante registrar en forma adecuada cada etapa del proceso de administración de riesgos, deberían registrarse las presunciones, hipótesis, métodos, fuentes de datos, análisis, resultados y razones para las decisiones.

La administración de riesgos puede ser aplicada a muchos niveles en una organización, ya sea a nivel estratégico o a niveles tácticos y operacionales. Puede ser aplicado a proyectos específicos, para sustentar decisiones específicas o para administrar áreas de riesgo reconocidas. Para cada etapa del proceso deberían mantenerse registros adecuados.

3. MODELO PARA LA GESTIÓN ESTRATÉGICA DE LOS RECURSOS TECNOLÓGICOS

3.1. Trayectorias tecnológicas sectoriales

Las organizaciones, dependiendo de la orientación del negocio, difieren en sus regímenes tecnológicos. Cada sector involucra distintas tecnologías, cada una de las cuales presenta una ruta histórica de desarrollo diferente y unos requerimientos estratégicos particulares. Es por ello que existe una gran dificultad para establecer un marco de aplicación general que integre la tecnología en el análisis estratégico y que contemple eficazmente la diversidad corporativa y sectorial.

El crecimiento y evolución de las empresas están inmersos en su dinámica innovadora. Dicha evolución se plasma en ciclos que a su vez marcan la pauta de trayectorias cimentadas en la tecnología; es decir que el proceso de nacimiento, crecimiento, madurez y declive de las distintas industrias y tecnologías son temas vinculados con el crecimiento de las empresas, las industrias, las regiones y los países.

Las organizaciones pueden verse sorprendidas en cualquier momento por la aparición de nuevos productos, nuevas tecnologías, nuevos competidores o cambios en los gustos de los clientes, que pueden amenazar seriamente la buena marcha de la empresa. La historia de la industria está llena de ejemplos de empresas, o incluso sectores completos que sucumbieron ante la súbita aparición de una nueva tecnología. La mayoría de los fabricantes de tubos de vacío, por ejemplo, no sobrevivió a la aparición del transistor.

La trayectoria tecnológica considera procesos de acumulación de conocimientos, de capacidades y de recursos, por lo que los pasos de esfuerzos pasados repercutirán en los resultados futuros. Los sociólogos, historiadores y economistas para referirse al proceso de innovación suelen emplear otros términos que reflejan la idea de flujo, como: cambio tecnológico, progreso técnico, desarrollo tecnológico o simplemente innovación. Los economistas industriales descomponen el proceso de innovación tecnológica en una secuencia de tres fases: invención, innovación y difusión.

Las organizaciones con más éxito se caracterizan por desempeñar actividades de explotación que derivan en nuevos productos y procesos mejorados, mientras exploran nuevas trayectorias y oportunidades que incrementarán sus capacidades tecnológicas futuras. Sin embargo, las organizaciones pequeñas o con recursos limitados para la innovación pueden encontrarse con barreras para combinar estas actividades de manera apropiada.

Las alianzas en las organizaciones son comunes en muchos sectores y se han convertido en una decisión estratégica para cualquier empresa. En las actividades tecnológicas, las redes y alianzas son una de las principales fuentes de innovación. Las alianzas tecnológicas impulsan la capacidad innovadora de la empresa a través de la combinación efectiva de los recursos de los socios.

Las soluciones temporales sirven de guía para un progreso técnico continuo que es válido hasta que se alcanza y se acepta una solución superior.

La trayectoria tecnológica ha sido enmarcada a partir del análisis de la innovación tecnológica. Dicha trayectoria está relacionada con el ciclo de la vida de la organización. Este fenómeno es un proceso complejo y evolutivo del

que no solo la dimensión tecnológica forma parte, sino también otras como las del mercado y de la producción. Dependiendo de los indicadores utilizados en su medición, la trayectoria tecnológica puede ser diferente.

Una innovación radical da lugar a la aparición de un nuevo producto, capaz de sustentar el desarrollo de una nueva industria; hay un período inicial de intensa innovación y optimización, hasta lograr la aceptación del producto en el segmento correspondiente del mercado. La interacción con el mercado pronto determina la dirección de las mejoras, que a menudo definen un diseño dominante.

A medida que crecen los mercados se registran innovaciones incrementales sucesivas para mejorar la calidad del producto, la productividad del proceso y la situación de los productores en el mercado. Se culmina en la madurez cuando la nueva inversión en innovaciones tiene rendimientos decrecientes. Según la importancia que tenga el producto, todo el proceso puede durar unos pocos años o varios decenios. Las mejoras suelen ser modelos sucesivos.

Las organizaciones de base científica y proveedores especializados y los resultados de innovación dependen de las actividades de investigación y desarrollo generados internamente, de modo que la gestión estratégica de los recursos tecnológicos se erige como una dimensión crítica.

El rendimiento del proceso innovador se relaciona con la ejecución eficaz de una gran diversidad de actividades tales como la selección y gestión de proyectos, la canalización de las necesidades del mercado, el diseño de la cartera tecnológica, la selección de los medios de protección del conocimiento, entre otro.

El desarrollar un conjunto integrado de rutinas garantiza la construcción de competencias dinámicas distintivas de innovación, que permiten a las empresas introducir nuevos productos o tecnologías de procesos más velozmente que la competencia.

3.2. Dirección estratégica de la tecnología

La dirección estratégica de la tecnología supone la implantación en la organización de los instrumentos de gestión necesarias para responder a la complejidad y la incertidumbre estructural en que se desenvuelve actualmente la empresa, dentro de un entorno cambiante que le exige una integración de la tecnología en su estrategia.

La tecnología ha abierto nuevos mercados y creado oportunidades para las empresas en crecimiento, al mismo tiempo que ha disminuido la dimensión de la brecha entre las empresas grandes y las pequeñas. Sin embargo, hay muchas empresas que utilizan la tecnología solo para cubrir sus necesidades diarias y no la utilizan plenamente como parte de su estrategia de negocios.

La organización deberá integrar en su plan estratégico sus estrategias tecnológicas y los cursos de acción necesarios para llevarlas a cabo.

La gestión estratégica de la tecnología le permite a la organización anticipar la evolución y desarrollo que la tecnología va a experimentar. Hace que se considere a esta como un activo empresarial que se puede gestionar y no como una variable externa. Permite asegurar la congruencia entre las inversiones en tecnología y las estrategias de negocio y corporativa, optimizando así los recursos de la empresa.

El éxito de una empresa intensiva en la tecnología depende de manera decisiva de su base tecnológica, es decir, de su capacidad para explorar y explotar la tecnología como una competencia medular, incorporar tecnología más avanzada en productos y servicios, y hacerlo en un período menor, con costos inferiores y con mayor rendimiento que los competidores.

El papel esencial que pasa a desempeñar la tecnología dentro del pensamiento estratégico se debe básicamente a la constatación de una serie de realidades, un entorno crecientemente competitivo, una reducción de los costos de la tecnología unida a un incremento de sus prestaciones y al hecho de que toda actividad en la empresa, ya sea acción o decisión, tiene un componente de información.

La importancia estratégica de la tecnología para la organización varía de unos sectores a otros, e incluso dentro de una misma compañía a lo largo del tiempo; así para algunas empresas la tecnología tiene un alto valor estratégico, mientras que en otras se le percibe simplemente como un soporte administrativo en el tratamiento de los datos.

El éxito o el fracaso de una organización se determinan por la rentabilidad de la industria a la que pertenece y su posición competitiva, o habilidad para conseguir ventajas sostenibles frente a los competidores, la tecnológica puede ayudar a una empresa a obtener ventajas competitivas. En la medida en que la tecnología afecte a las actividades de valor de la organización y cambie sus relaciones con ellas, transformando su ámbito de competencia o reformando el modo en que los productores cubren las necesidades de los clientes, esta pasará progresivamente a utilizarse en el plano estratégico.

La mayoría de las organizaciones presentan una estructura organizativa que refleja el flujo de información que se produce dentro de ellas. A medida que la tecnología crea más tareas funcionales y rutinarias, y compartiendo el acceso a la información, también permite que surjan nuevas formas organizativas.

3.2.1. Análisis estratégico

El análisis estratégico requiere que mediante el análisis externo se detecten las oportunidades y amenazas a las que la empresa se enfrenta como consecuencia de las situaciones del entorno en el que opera; es necesario efectuar el análisis interno de los recursos y competencias que la empresa posee; así también un diagnóstico y evaluación de sus recursos. La combinación de los análisis externo e interno se llama análisis Foda, el cual es un examen de fortalezas, oportunidades, debilidades y amenazas de la organización

- Análisis externo: el propósito es identificar oportunidades y amenazas estratégicas en el ambiente operativo de la organización que influirán en la manera en que se cumple su misión. Aquí se encuentran las oportunidades (tendencias positivas en los factores del ambiente externo), y las amenazas (tendencias negativas en los factores del ambiente externo). Se centra en el estudio de la información derivada de diversos aspectos como: los sistemas de patentes, la evaluación de las nuevas tecnologías, la confección y estudio del ciclo de vida de las tecnologías, etc.. Prácticamente se deben examinar tres ambientes interrelacionados: el inmediato a ambiente de la industria en el que opera la organización, el ambiente nacional o del país, y el más amplio, el socioeconómico y macroambiente.

Debido a que muchos mercados ahora son globales, el análisis del ambiente de la industria también implica evaluar el impacto de la globalización en la competencia dentro de una industria. Se pretende determinar el marco estratégico de la empresa evaluando el papel estratégico de las distintas tecnologías que conforman el sistema tecnológico vigente, considerando tanto los efectos de estas tecnologías sobre la estructura de la competencia, como sobre las propias actividades de la empresa.

- Análisis interno: este sirve para aislar las fuerzas y debilidades de la organización. Aquí se consideran aspectos tales como identificar la cantidad y la calidad de recursos y capacidades de una compañía y las maneras de construir habilidades únicas y distintivas o específicas de la compañía, cuando se examinan las fuentes de la ventaja competitiva. La empresa debe lograr un nivel superior en la eficiencia, calidad, innovación y atención al cliente. Las fortalezas de la organización conducen a un desempeño superior.

  Con el análisis interno tiene como fin la modelización del contenido tecnológico de todas las actividades de la cadena de valor de la empresa, y pretende detectar sus fortalezas y debilidades frente a sus competidoras. Aquí se encuentran las fuerzas (actividades que la organización hace bien o recursos exclusivos), las debilidades (actividades que la organización no hace bien o recursos que no tiene), y las capacidades centrales (principales destrezas, habilidades y recursos que crean valor para la organización y que determinan sus armas competitivas.

Persigue indicar cómo a cada actividad concreta de la cadena de valor, tanto a las primarias como a las de apoyo, se le puede asociar una tecnología determinada que puede ser generadora de ventajas en costos o en diferenciación, capaces de mejorar la posición competitiva de la empresa. Las áreas funcionales de todas las organizaciones tienen fuerzas y debilidades, independientemente de sus áreas. Las fuerzas y debilidades internas, sumadas a las oportunidades y amenazas externas, así como un enunciado claro de la visión y misión, son la base para establecer objetivos y estrategias.

- Diagnóstico y evaluación: consiste en la realización de un inventario de los recursos tecnológicos de la empresa, de su patrimonio tecnológico, así como la evaluación de su potencial, esto es, de su posible impacto competitivo. Ayudará a resolver problemas operativos al conocer la interrelación entre los sistemas tecnológicos y sus procesos de negocios. La caracterización de cada tecnología dependerá, esencialmente, del papel que desempeñe dentro de cada actividad emprendida por la organización

3.2.2. Diseño de la estrategia tecnológica

Sobre la base de datos de los resultados del análisis estratégico, del diagnóstico tecnológico y de la evaluación del patrimonio tecnológico, en el diseño de la estratégica hay que considerar tres acciones: elección de las tecnologías que hay que desarrollar, diseño de la cartera tecnológica y elección del momento para la introducción de nuevas tecnologías.

- Elección de las tecnologías que hay que desarrollar: la elección de las tecnologías sobre las que la organización desarrollará sus actuaciones es

una consecuencia directa de sus estrategias, de la medida en que las distintas tecnologías contribuyen al logro de los objetivos empresariales; es un punto de partida del proceso de dirección estratégica de la tecnología. Con la elección de la tecnología se tiene que ejercer el mayor impacto; con eso se constituye la fuerza conductora de la competencia y la fortaleza de la organización. Su dominio se convierte en una cualidad distintiva e indispensable, necesaria para aquellas empresas que quieren alcanzar el éxito en un determinado proyecto.

En la elección de la tecnología se tiene que evaluar la oportunidad, escalabilidad, estabilidad, disponibilidad de los recursos técnicos y financieros. Además del presupuesto de capital, hay que tener en cuenta la compatibilidad con la estructura organizativa y métodos de trabajo existentes. La elección no se puede considerar como una sola acción, sino un proceso que incluya la investigación tecnológica continua, la elección de tecnologías adecuadas y la implantación de la elegida, todo ello con el apoyo y asesoramiento especializado.

- Diseño de la cartera tecnológica: se trata de elegir las vías para el acceso a las nuevas tecnologías, determinando el modo en que la organización obtendrá la tecnología necesaria. La tecnología es fundamental para alcanzar los objetivos de la organización, prestar un mejor servicio y mejorar los procesos; por lo que es de vital importancia el diseño de la cartera tecnológica en el entorno de la empresa. Para el diseño de la cartera tecnológica se pueden realizar con los siguientes pasos:

    - Inversión de tecnología propia: persigue la obtención del mayor beneficio posible de los recursos tecnológicos y potenciales de la

organización. Trata de una actuación ofensiva, propia de una dirección emprendedora y creativa que busca la optimización de sus tecnológicas. Invertir en tecnología propia es invertir en la propia independencia.

- Enriquecimiento tecnológico: mediante la inversión en tecnología propia y ajena se atenderá el objetivo de enriquecimiento tecnológico, que pretende incrementar el patrimonio tecnológico, o mantener su valor. El enriquecimiento tecnológico no consiste en desarrollar todos los recursos internamente, sino en que la empresa sepa cómo, dónde y cuándo obtener dichos recursos de fuentes externas.

- Una estrategia para enriquecer el patrimonio tecnológico debe basarse en examinar las posibilidades externas antes de decidirse por realizar el desarrollo internamente; se trata de ahorrar tiempo y esfuerzos, tratando de no inventar de forma propia lo que ya han inventado otros. Incluso se puede admitir que la empresa puede sobrevivir sin capacidad de generar tecnología internamente, pero necesita tener una red bien equipada de contactos externos, además de disponer de la capacidad necesaria para utilizar de forma eficaz la tecnología adquirida.

- Inversión en tecnología de terceros: se realiza con una adquisición que no se orienta al enriquecimiento tecnológico de la empresa, no tiene como objetivo el incremento del patrimonio tecnológico, sino la utilización inmediata de una tecnología cedida bajo licencia. Este tipo de inversión conlleva una fuerte dependencia de pagos de derecho

de utilización, por lo que su empleo como alternativa para la configuración de la cartera tecnológica debe limitarse al máximo.

- Protección de las tecnologías: se busca salvaguardar los derechos tecnológicos logrados por la organización, utilizando como herramientas los diversos mecanismos legales de regulación de la propiedad. Esta actividad termina con una correcta organización del almacenamiento, transmisión y reparto de los conocimientos tecnológicos de la empresa.

- Elección del momento para la introducción de las nuevas tecnologías: esta elección depende de la actitud de la organización respecto de la innovación. Es una decisión asociada a la formulación de las estrategias de innovación, hay que analizar sus relaciones con las estrategias tecnológicas. La introducción de nuevas tecnologías en la organización puede contribuir a la aparición de nuevos modos de trabajo y a la eliminación de tareas aburridas y rutinarias, introduciendo una mayor variedad de habilidades necesarias en el puesto de trabajo y permitiendo a los trabajadores desempeñar trabajos de mayor responsabilidad y más retadores.

  La introducción de una nueva tecnología en el contexto de trabajo produce también cambios en la estructura y el funcionamiento de los grupos de trabajo. El impacto es previsible sobre redes de comunicación, flujos de información, eficiencia de la comunicación, patrones de interacción grupal, toma de decisiones, emergencia de liderazgo y formación de coaliciones.

3.2.3. Implantación de la estrategia tecnológica

Una vez definidas con precisión las estrategias tecnológicas, se requiere su implantación y puesta en funcionamiento; se pueden mencionar los siguientes pasos:

- Asignación de recursos para las actividades tecnológicas: es necesario elaborar un presupuesto mediante el cual se asignen los fondos necesarios para la ejecución de cada proyecto. Su confección es una tarea ardua y difícil, y para su elaboración puede recurrirse a diversos procedimientos. La elaboración y aprobación del presupuesto dentro de la organización ayudan a que se logren proyectos de inversión en actualización tecnológica, ampliación de la capacidad instalada, integración de intereses accionarios y expansión de los mercados. El presupuesto solo es un estimado, no pudiendo establecer con exactitud lo que sucederá en el futuro. Es importante para los directivos tener de antemano una perspectiva de los planes del negocio para un período suficientemente largo, y no se concibe sin la formulación de presupuestos para períodos cortos, con programas detallados para el periodo inmediato siguiente.

- Diseño de la estructura de la organización: la implantación y desarrollo de la estrategia tecnológica precisa de las modificaciones necesarias en la estructura organizativa, con la finalidad de facilitar la comunicación y permitir el desarrollo entre las áreas. El diseño organizacional es el proceso de gestión de la estructura de la organización para que esta pueda realizar y coordinar las acciones necesarias para alcanzar sus metas. El comportamiento de la empresa es el resultado del diseño y de los principios que subyacen en su operación.

Hay que destacar que entre más pequeña sea la organización, mayor será el impacto de las tecnologías en su estructura, así como cuanto más grande sea la organización, el efecto será menor. Un cambio tecnológico en una pequeña o mediana empresa repercutirá fuertemente en la estructura, ya que cambia el proceso productivo, los requerimientos de habilidades de los trabajadores para los puestos de trabajo, la cantidad de mano de obra necesaria y los ritmos de producción.

El diseño organizacional es muy importante debido a la creciente presión competitiva, globalización y manejo más abierto de la tecnología de la información, el diseño organizacional se ha convertido en una de las prioridades más importantes para las organizaciones. El diseño organizacional tiene implicaciones esenciales en la capacidad de la organización para enfrentar contingencias y lograr una ventaja competitiva sustentable.

El diseño organizacional define la estructura de una organización, factor de apoyo clave para la cadena de valor, la cual permite saber qué partes crean valor y cuáles no. No hay estructuras buenas o malas, cualquier alternativa de disposición de las unidades de una empresa tiene la capacidad de responder a los requerimientos de su razón de ser y de integrarse a los cambios de escenario en que se vaya insertando conforme su ciclo de vida y oportunidades de la organización se lo exija.

- Gestión de los proyectos: la implantación de las estrategias tecnológicas supone la ejecución por parte de la organización, de actividades que se llevan a cabo mediante la ejecución de proyectos. Estos se configuran como un conjunto de actividades no repetitivas, efectuadas por técnicos y especialistas de diferentes áreas y grupos de trabajo, que deben

realizarse dentro de unos costos y plazos fijados, hasta conseguir especificaciones, prestaciones o resultados predeterminados.

El tratamiento de los proyectos y su gestión son complejos y exige, por una parte, la clasificación de los proyectos, su posterior evaluación y selección, así como el seguimiento de la ejecución de los mismos; para lo que se requiere la aplicación de técnicas que permitan una optimización de la cartera de la empresa. La gestión del proyecto incluye la planificación, organización, ejecución, seguimiento y control de todas las actividades para la realización del proyecto, donde el éxito del proyecto radica en los beneficios e impactos que deben ser evaluados de acuerdo con sus objetivos en términos de mercado, económicos, sociales, ambientales y recursos tecnológicos.

La gestión de proyectos de tecnología es una poderosa herramienta que se debe enmarcar dentro de los procesos generales de innovación al que está sometida la organización. Tiene una gran importancia, puesto que se requiere un adecuado control de los recursos necesarios para las diferentes etapas de desarrollo de un proyecto, para que se garantice que se tendrán las condiciones para el logro de los objetivos. Entre las mejores prácticas a la hora de gestionar un proyecto tecnológico se pueden mencionar las siguientes actividades:

- Definir el alcance y los objetivos del proyecto: es muy importante entender los objetivos del proyecto, para poder determinar los objetivos reales para planificar el proyecto.

- El alcance o área de competencia define los límites del proyecto: se define qué es lo que está dentro o fuera de los límites del proyecto;

dicha actividad determinará la cantidad de trabajo que se necesita realizar.

- Definir las tareas: definir qué tareas se esperan del proyecto y documentarlas con suficiente detalle para que cualquiera de los involucrados pueda llevarla a cabo correcta y eficientemente.

- Planificar el proyecto: se requiere que el director de proyecto decida qué personal, recurso y presupuesto se necesita para completar el mismo. El equipo del trabajo debe estar involucrado en la estimación de la duración de las actividades, establecer hitos que indiquen fechas críticas durante el desarrollo del proyecto y escribirlas en la planificación.

- Comunicación: la planificación resulta inútil si no se comunica efectivamente al equipo del proyecto, porque el grupo de trabajo no sabe cuáles son las actividades que les corresponde.

- Seguimiento y reporte de avance del proyecto: una vez que el proyecto se encuentre en ejecución debe ser monitoreado y se tiene que comparar el progreso actual con el proyecto. Se deben registrar las variaciones entre lo real y lo proyectado, como el costo, cronograma y alcance.

- Gestión del cambio: administrar los cambios; el director de proyecto puede tomar decisiones sobre si incorpora o no los cambios inmediatos o en el futuro, o directamente rechazarlo.

- Gestión del riesgo: los riesgos varían con cada proyecto pero se deben identificar lo antes posible, en forma particular.

3.2.4. Control estratégico

El proceso de dirección estratégica de la tecnología se cierra con el control estratégico, mediante el cual se diseñan y aplican los mecanismos necesarios para asegurar el éxito de dicho proceso, a la vez que proporcionan una valiosísima información para la siguiente ronda del ciclo de planificación.

El control estratégico tratará de facilitar el seguimiento de las acciones internas y externas de la organización, las cuales le van a permitir alcanzar los objetivos deseados con base en las estrategias desarrolladas; es el encargado de supervisar cómo se comporta y cuán efectiva es la estrategia de la organización. En las pequeñas empresas la utilización de los instrumentos de control de gestión de una manera sencilla, va a facilitar las tareas referidas a la implantación de un control estratégico.

Todo sistema de control mide, corrige, verifica y planea, sin embargo en el sistema de control estratégico, cuyo objetivo está enfocado en el futuro, sugiere los elementos para una nueva definición. Los controles ofrecen los parámetros que servirán para aplicar las estrategias y las medidas correctivas que se tomarán cuando se requieren ajustes relacionados con su aplicación.

El control estratégico tiene que verificar la validez de las hipótesis clave, acerca de la evolución de la empresa y su entorno, sobre las que descansa la formulación de la estrategia. Si los empleados y directivos de la organización han implementado bien la estrategia, un eventual fallo en la consecución de los

resultados esperados, indica que la teoría incorporada a la estrategia puede no ser válida.

La actividad del control está centrada en controlar si la estrategia se está llevando a cabo como se planificó y si los resultados obtenidos son los esperados, introduce a la estrategia dentro de las acciones a realizar por la organización.

Un sistema de control estratégico debe establecer en el presente una guía cualitativa y cuantitativa, tanto para el logro del objetivo de mejoramiento y desarrollo continuo de las personas, como para el logro de los objetivos estratégicos de la organización considerada como un todo.

En el control estratégico a diferencia del control de gestión, la verificación de los resultados tiene como propósito fundamental la identificación de los problemas relacionados con el logro de los objetivos y el análisis de sus causas y efectos, para diseñar las acciones correctivas que garanticen la buena marcha hacia el futuro. Evaluar las estrategias se centra en examinar los resultados reales con las metas esperadas, para luego apoyarse en toma de acciones correctivas que garanticen concordancia con lo planeado. Las acciones revisadas pueden incluir el replanteamiento de las tácticas y de ser necesario, la misión de la organización.

3.3. Ciclo de mejora

Es una estrategia de mejora continua de la calidad en cuatro pasos: planificar, implantar, verificar y actuar, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los sistemas de gestión de calidad.

El ciclo de mejora se inicia con la definición del propósito y alcance del sistema o proceso que se desea mejorar, teniendo como marco un diagnóstico y medición de línea base que determina el estado real del proceso.

La interpretación de este ciclo es de la siguiente manera: cuando se busca obtener algo, lo primero que hay que hacer es planificar cómo conseguirlo, después se procede a realizar las acciones planificadas (hacer); a continuación se comprueba qué tal se ha hecho (verificar) y finalmente se implementan los cambios pertinentes para no volver a incurrir en los mismos errores (actuar). Nuevamente se empieza el ciclo planificando su ejecución, pero introduciendo las mejoras provenientes de la experiencia anterior.

Los resultados de la implementación de este ciclo permiten a las organizaciones una mejora integral de la competitividad y de los productos y servicios, mejorando continuamente la calidad, reduciendo los costos, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad de la empresa u organización.

El ciclo de mejora es tan poderoso para incrementar los rendimientos de la organización, donde se trata de que toda una organización adopte la cultura del ciclo, lo que implica trabajo real en equipo; eso necesita comunicaciones eficaces, valores, visión, espacio y tiempo.

3.3.1. Planificar

Es la primera etapa del ciclo de mejora de la tecnología, comienza con una definición del problema tecnológico y la recopilación de los datos necesarios para su análisis.

Se trata de responder preguntas básicas en relación con las tecnologías: ¿qué hacer?, ¿qué tecnologías seleccionar y desarrollar?, ¿cómo hacerlo? y ¿cómo desarrollar las tecnologías?, implica la realización de dos actividades:

- Elaboración de la matriz de planificación estratégica de la tecnología: se utiliza para inventariar las tecnologías o competencias tecnológicas de la empresa y ponerlas en relación con los objetivos que esta tiene, expresados mediante los ítems de control de negocio de la dirección, así como por los productos que quiere desarrollar. Esta matriz permite priorizar las tecnologías que se deben desarrollar para alcanzar los objetivos empresariales; para realizarlo se detallan los pasos siguientes:

    - Incorporación de los objetivos de la organización, expresados por medio de los ítems de control del negocio y la relación de productos que se pretenden obtener o desarrollar.

    - Elaboración del inventario tecnológico de la organización.

    - Determinación de la relación entre las tecnologías y los objetivos.

    - Incorporación de los criterios de evaluación correspondiente a los objetivos de la organización, tales como: situación actual, dificultad que entraña su mejora, objetivo respecto de la situación actual e importancia estratégica.

    - Priorización de las tecnologías en función de su contribución a los diferentes objetivos de la organización; para ello se multiplica la importancia o prioridad de cada objetivo en función de la relación existente entre cada tecnología y objetivo. La suma de los valores

correspondientes a cada tecnología proporcionarán la puntuación total de la misma que permite su priorización.

- Asignación de recursos para el desarrollo de cada una de las tecnologías evaluadas.

- Elaboración de la matriz de priorización de acciones de vigilancia tecnológica y proyectos: se utiliza para el diseño de la cartera tecnológica y define la relación entre las acciones de vigilancia tecnológica y los proyectos, y las tecnologías o competencias tecnológicas que la organización ha priorizado en función de sus objetivos. Para realizarlo se detallan los pasos siguientes:

  - Incorporación de las tecnologías priorizadas por medio de la matriz de planificación estratégica de la tecnología.

  - Elaboración del inventario de acciones de vigilancia tecnológica y proyectos a ejecutar por la organización.

  - Determinación de la relación entre tales acciones de vigilancia tecnológica, proyectos y las tecnologías priorizadas, indicando mediante símbolos su carácter fuerte, medio o débil.

  - Incorporación de los criterios de evaluación correspondientes a las tecnologías, tales como: fortaleza, estado evolutivo, dificultad y riesgo de su desarrollo e importancia o prioridad.

  - Priorización de las acciones de vigilancia tecnológica y proyectos a ejecutar por la organización, en función de su contribución al

desarrollo de las tecnologías; para ello se multiplica la importación o prioridad de cada tecnología para la relación existente entre cada acción. La suma de los valores correspondientes a cada acción o proyecto proporcionará la puntuación total de acciones que permite su priorización.

- Asignación de recursos para el desarrollo de cada una de las acciones de vigilancia tecnológica y proyectos a ejecutar por la organización.

3.3.2. Implantar

Constituye la segunda etapa del ciclo de mejora de la tecnología. Consiste en ejecutar lo planificado, por lo que es necesario realizar las siguientes actividades:

- Lanzamiento de las acciones de vigilancia tecnológica: a partir de las prioridades establecidas en la etapa anterior, una vez que han sido asignados los recursos del presupuesto a las diferentes acciones de vigilancia tecnológica y proyectos, se adoptan las medidas de carácter organizativo necesarias para su desarrollo, se abordan las acciones formativas que se consideran precisas para el éxito de las acciones y proyectos, y se inicia su ejecución.

- Gestión de las acciones de vigilancia tecnológica: consiste en la ejecución y seguimiento de todas las actividades relativas a la cartera tecnológica de la empresa.

3.3.3. Verificar

Tercera etapa del ciclo de mejora de la tecnología. A través de la medición de los resultados obtenidos en la etapa anterior se pretende dar contestación a la pregunta ¿las cosas pasaron según se planificaron?, en este punto es preciso revisar todas y cada una de las actividades que se realizaron, así como en su implantación y ejecución.

Se evalúan los resultados reales conseguidos y se comparan con los objetivos establecidos en la planificación. La clave de la verificación está en haber determinado con anterioridad indicadores para la medición de los objetivos.

3.3.4. Actuar

El ciclo de mejora de la tecnología se cierra con esta etapa en la que plantea ¿cómo mejorar la próxima vez?, para responder a ello es necesario tomar las acciones pertinentes que procuren una mejora continua, realimentando el comienzo de una nueva vuelta en el ciclo; este tiene un carácter iterativo de forma que puede convertirse en un proceso continuo de mejora sostenida.

En esta etapa, la evaluación de las tecnologías, la valoración del impacto competitivo de las acciones y proyectos desarrollados, la efectividad de los mecanismos de protección de las tecnologías y los resultados de su explotación, proporcionan las entradas para reiniciar una nueva vuelta en el ciclo con una planificación adecuadamente corregida.

Con base en las conclusiones del paso anterior se elige una de las siguientes opciones:

- Si se han detectado errores parciales en el paso anterior, realizar un nuevo ciclo con nuevas mejoras.

- Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos.

- Si se han detectado errores insalvables, abandonar las modificaciones de los procesos.

- Ofrecer una retroalimentación y/o mejora en la planificación.

CONCLUSIONES

1. Los recursos tecnológicos son una herramienta en donde se hace uso de la tecnología para cumplir con su propósito y sirven para optimizar procesos, tiempos y recursos humanos dentro de la organización.

2. El control es un factor importante para el logro de los objetivos de la organización y por ello debe reunir ciertas características para ser efectivo. El control deberá ajustarse a las necesidades de la empresa y al tipo de actividad que se desee controlar. Los buenos controles deben relacionarse con la estructura organizativa y reflejar su eficacia.

3. Los recursos tecnológicos con que cuenta la organización deben ser utilizados para apoyar a alcanzar los objetivos, por lo que hay que hacer buen uso de los mismos de forma eficaz y eficiente.

4. Los recursos tecnológicos puestos a disposición de los empleados de la organización deben garantizar la seguridad, disponibilidad, fiabilidad y privacidad de las comunicaciones, así como también deben preservar la privacidad de los empleados. Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, finanzas, entre otro; los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

5. La utilización de tecnología de información específicamente computadoras y ordenadores electrónicos para el manejo y procesamiento de información en la captura, almacenamiento, protección y recuperación de datos e información, contribuye para la obtención de los objetivos del negocio.

6. Para garantizar que los objetivos de la empresa serán alcanzados es necesario tener controles que ayudan a reducir los riesgos o amenazas que pueden tener un impacto negativo sobre los activos, procesos u objetivos de la organización.

7. El crecimiento y evolución de la organización están inmersos en su dinámica innovadora. Dicha evolución se plasma en ciclos que a su vez marcan la pauta de trayectorias cimentadas en la tecnología; es decir que el proceso de nacimiento, crecimiento, madurez y declive de las distintas industrias y tecnologías son temas vinculados con el crecimiento de las empresas y las industrias; por lo tanto es importante que la organización tenga un plan de administración y actualización de hardware y software.

8. El riesgo a nivel de tecnología, se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una pérdida, por ejemplo el riesgo de perder datos debido a rotura de disco o virus informáticos. Las consecuencias de la materialización de amenazas se asocian a un determinado nivel de impacto en función de multitud de factores (pérdidas económicas efectivas, pérdida de conocimiento y de competitividad, interrupción de negocio, pérdida de imagen, entre otro.).

RECOMENDACIONES

1. Las organizaciones deben de innovar para ser más eficientes en sus procesos en la utilización de recursos tecnológicos, y así tener mejores oportunidades y ser más competitivos.

2. Las organizaciones deben de contar con controles sobre los recursos tecnológicos, humano e información, para protegerlos y buscar una adecuada administración ante riesgos potenciales que puedan afectar las operaciones de la empresa, para garantizar la correcta ejecución de las funciones y actividades del negocio.

3. La organización debe de tener políticas de uso y seguridad de los recursos tecnológicos; las cuales deben de ser cumplidas por los usuarios que utilicen cualquiera de las herramientas informáticas, comunicación e información.

4. Las organizaciones tienen que controlar sus recursos tecnológicos y humanos para rectificar que las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas se estén llevando a cabo, para prevenir situaciones no deseadas que puedan interferir en el alcance de los objetivos de la empresa.

5. Para que la tecnología de información pueda contribuir a la obtención de los objetivos de la organización, tiene que evaluar la oportunidad, escalabilidad y disponibilidad de los recursos técnicos y financieros al

momento de elegir una tecnología, ya que de ahí la empresa desarrollará sus acciones.

6. Las organizaciones deben realizar estudios de riesgos sobre sus activos para garantizar que los objetivos serán alcanzados, ya que los activos son vulnerables hacia una amenaza y ponen en peligro la confidencialidad, integridad, disponibilidad del mismo, causando daños o perjuicios a la empresa.

7. Las organizaciones deben contar con un ciclo de mejora en tecnología para incrementar el rendimiento de la empresa, priorizando la que se debe desarrollar, adquirir y actualizar, para alcanzar los objetivos empresariales.

8. Es necesario que la organización tenga conocimiento sobre los recursos tecnológicos que impactan en el crecimiento de la empresa, el éxito o el fracaso, determinándolo por la rentabilidad de la industria a la que pertenece y su posición competitiva o habilidad para conseguir ventajas sostenibles frente a los competidores; la tecnológica puede ayudar a la empresa a obtener ventajas competitivas.

BIBLIOGRAFÍA

1. Alegsa. *Diccionario de Informática*. [en línea]. <http://www.alegsa.com.ar>. [Consulta: 12 de febrero de 2015].

2. ARREDONDO MORALES, Perla Azucena. *Servidores web*. [en línea]. <http://www.monografias.com/trabajos75/servidores-web/servidores-web.shtml>. [Consulta: 12 de febrero de 2015].

3. CABRERA, Elibeth. *Control*. [en línea]. <http://www.monografias.com/trabajos14/control/control.shtml>. [Consulta: 10 de febrero de 2015].

4. Cyberprimo. *Servidores: qué son y para qué sirven*. [en línea]. <http://www.cyberprimo.com/2010/02/servidores-que-son-y-para-que-sirven.html>. [Consulta: 10 de febrero de 2015].

5. Definición de internet. [en línea]. <http://www.definicion.org/internet>. [Consulta: 12 de febrero de 2015].

6. Definición de regulación. [en línea]. <http://definicion.de/regulacion/>. [Consulta: 12 de febrero de 2015].

7. Ergo Laboris. *Metodología para la evaluación de riesgos laborales*. [en línea].<http://www.ergolaboris.com/docs/Documents_tecnics/Metodologia_Evaluacion_Riesgos_Laborales.pdf>. [Consulta: de 14 de febrero de 2015].

8. GÓMEZ. *Análisis de Riesgo*. [en línea]. <http://www.monografias.com/trabajos83/analisis-riesgo/analisis-riesgo.shtml>. [Consulta: 15 de febrero de 2015].

9. GONZÁLEZ, Pilar. *Introducción al proceso de gestión de riesgos de TI* [en línea]. <http://www.seinhe.com/blog/52-introduccion-al-proceso-de-gestion-de-riesgos-de-ti>. [Consulta: 14 de febrero de 2015].

10. HILLSON, David. *Problemas con la probabilidad*. [en línea]. <http://www.risk-doctor.com/pdf-briefings/risk-doctor29s.pdf>. [Consulta: 14 de febrero de 2015].

11. Informática hoy. *Seguridad informática - virus – antivirus*. [en línea]. <http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Que-es-un-antivirus.php>. [Consulta: 11 de febrero de 2015].

12. Instituto Internacional de Administración de Riesgos, S. A. de C. V. *Administración de riesgos*. [en línea]. <http://seguridadindustrial.com.mx.dish14.net.ibizdns.com/Biblioteca/ADMON.%20DE%20RIESGOSAUSTRALIANO%20NEO%20ZELANDES.pdf>. [Consulta: 15 de febrero de 2015].

13. Jornada Nacional de Seguridad Informática. *Análisis y gestión de riesgos, base fundamental del SGSI caso: Metodología MAGERIT*. [en línea]. <http://www.acis.org.co/fileadmin/ Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGes

tionSeguridadInformacionCasoMagerit.pdf>. [Consulta: 15 de febrero de 2015].

14. Laboratorio de redes y seguridad. *Tutorial de seguridad Informática*. [en línea].<http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi /Cap5.html>. [Consulta: 15 de febrero de 2015].

15. Mis respuestas. *Diccionario*. [en línea]. <http://www.Misrespuestas .com/computadoras.html>. [Consulta: 10 de febrero de 2015].

16. Monster. *Amenazas informáticas*. [en línea]. <http://consejos-empleo.monster.es/trucos-busqueda-empleo/como-empezar/amenazas-informaticas/article.aspx>. [Consulta: 14 de febrero de 2015].

17. *Ordenadores y portátiles. Cables de red*. [en línea]. <http://www. ordenadores-y-portatiles.com/cables-de-red.html>. [Consulta: 13 de febrero de 2015].

18. Pergamino virtual. *Telnet*. [en línea]. <http://www.pergaminovirtual.com .ar/definicion/Telnet.html>. [Consulta: 12 de febrero de 2015].

19. PINO, Diego. *Los Sistemas de Bases de Datos Relacionales (RDBMS)*. [en línea]. <http://diegopino.blogspot.com/2009/03/los-sistemas-de-bases-de-datos.htm>. [Consulta: 12 de febrero de 2015].

20. Real Academia Española. *Diccionario de la Lengua Española*. [en línea]. <http://lema.rae.es/drae/>. [Consulta: 10 de febrero de 2015].

21. Secretaria de Control Interno. *Control*. [en línea]. <http://www.valledelcauca.gov.co/control/publicaciones.php?id=3425>. [Consulta: 10 de febrero de 2015].

22. Slide Share. *Concepto de riesgo*. [en línea]. <http://www.slideshare.net/cerodano/concepto-de-riesgo>. [Consulta: 14 de febrero de 2015].

23. TOBAR, Luis Roberto. *Análisis y administración de riesgos*. [en línea]. <http://innovaseguros.wordpress.com/2010/03/18/analisis-y-administracion-de-riesgos/>. [Consulta: 15 de febrero de 2015].

24. Wikimedia. *Enciclopedia libre*. [en línea]. < http://es.wikipedia.org/wiki/Wikipedia>. [Consulta: 10 febrero de 2015].

25. World Disaster Reduction Campaign. *Qué es el riesgo*. [en línea]. <http://www.unisdr.org/2004/campaign/booklet-spa/page9-spa.pdf>. [Consulta: 14 de febrero de 2015].